



PanoVu Series Network Camera

User Manual

User Manual

COPYRIGHT ©2019 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual

This Manual is applicable to PanoVu Series Network Camera.

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (<http://overseas.hikvision.com/en/>). Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE

USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED. SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES. IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable

harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of

equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific

battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information, see: www.recyclethis.info.

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Safety Instruction

These instructions are intended to ensure that the user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into 'Warnings' and 'Cautions':

Warnings: Serious injury or death may be caused if any of these warnings are neglected.

Cautions: Injury or equipment damage may be caused if any of these cautions are neglected.



Warnings:

- Please adopt the power adapter which can meet the safety extra low voltage (SELV) standard. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as an adapter overload may cause over-heating and can be a fire hazard.
- When the product is installed on a wall or ceiling, the device should be firmly fixed.
- To reduce the risk of fire or electrical shock, do not expose the indoor used product to rain or moisture.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Please install blackouts equipment into the power supply circuit for convenient supply interruption.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the product yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)
- Please do not look directly into the laser light within 6 meters because laser is hazardous to humans.



Cautions:

- Make sure the power supply voltage is correct before using the product.
- Do not drop the product or subject it to physical shock. Do not install the product on vibratory surface or places.
- Do not expose it to high electromagnetic radiating environment.
- Do not aim the lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the product.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor not be exposed to the laser beam.
- For working temperature, please refer to the specification manual for details.
- To avoid heat accumulation, good ventilation is required for a proper operating environment.
- While shipping, the product should be packed in its original packing.

Warnings Follow these safeguards to prevent serious injury or death.	Cautions Follow these precautions to prevent potential injury or material damage.

- Please use the provided glove when open up the product cover. Do not touch the product cover with fingers directly, because the acidic sweat of the fingers may erode the surface coating of the product cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the product cover. Do not use alkaline detergents.
- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufacturer recommended battery type.

Table of Contents

ABOUT THIS DOCUMENT	1
OVERVIEW OF CONTENTS	1
NOTICE	1
CHAPTER 1 ACTIVATING AND ACCESSING TO THE CAMERA	2
1.1 SYSTEM REQUIREMENT	2
1.2 ACTIVATING THE CAMERA	2
1.2.1 <i>Setting the Camera over the LAN</i>	2
1.2.2 <i>Activating the Camera</i>	3
1.3 SETTING THE CAMERA OVER THE WAN (OPTIONAL)	8
1.3.1 <i>Static IP Connection</i>	8
1.3.2 <i>Dynamic IP Connection</i>	9
1.4 ACCESSING TO THE CAMERA	10
1.4.1 <i>Accessing by Web Browsers</i>	10
1.4.2 <i>Accessing by Client Software</i>	11
1.5 POWER-UP ACTION	12
CHAPTER 2 SETTING LOCAL PARAMETERS AND NETWORK	13
2.1 CONFIGURING LOCAL PARAMETERS	13
2.2 CONFIGURING NETWORK SETTINGS	14
2.2.1 <i>Basic Settings</i>	14
2.2.2 <i>Advanced Settings</i>	19
CHAPTER 3 LIVE VIEW	28
3.1 INSTALL THE PLUG-IN	28
3.2 LIVE VIEW PAGE	29
3.2.1 <i>Descriptions of the live view page:</i>	29
3.2.2 <i>Live View Operation</i>	29
3.3 CONFIGURING IMAGE SETTINGS	33
3.3.1 <i>Configuring Display Settings</i>	33
3.3.2 <i>Configuring OSD Settings</i>	39
3.3.3 <i>Configuring Text Overlay Settings</i>	40
3.3.4 <i>Configuring Privacy Mask for Panoramic Camera Channel</i>	41
3.4 CONFIGURING VIDEO AND AUDIO SETTINGS	41
3.4.1 <i>Configuring Video Settings</i>	41
3.4.2 <i>Configuring Audio Settings</i>	43
3.4.3 <i>Configuring ROI Settings</i>	43
3.4.4 <i>Target Cropping</i>	45
CHAPTER 4 PTZ CONTROL	46
4.1 OPERATING PTZ CONTROL	46
4.1.1 <i>Setting/Calling a Preset</i>	46
4.1.2 <i>Setting/Calling a Patrol</i>	48
4.1.3 <i>Setting/Calling a Pattern</i>	49
4.2 PTZ CONFIGURATION	50

4.2.1	Configuring Basic PTZ Parameters	50
4.2.2	Configuring PTZ Limits	51
4.2.3	Configuring Initial Position	52
4.2.4	Configuring Park Action	53
4.2.5	Configuring Privacy Mask for PTZ Camera Channel	54
4.2.6	Configuring Scheduled Tasks	55
4.2.7	Clearing PTZ Configurations	57
4.2.8	Configuring PTZ Control Priority	57
4.2.9	Configuring Panorama Tracking	58
4.2.10	Rapid Focus	60
CHAPTER 5	STORAGE AND PLAYBACK.....	61
5.1	STORAGE SETTINGS.....	61
5.1.1	Configuring Net HDD	61
5.1.2	HDD Management.....	62
5.1.3	Configuring Record Schedule.....	63
5.1.4	Configuring Capture Schedule	66
5.1.5	Cloud Storage	67
5.2	PICTURE.....	67
5.3	PLAYBACK.....	68
5.3.1	Play Back Video Files	68
5.3.2	Downloading Video Files.....	70
5.3.3	Downloading Captured Pictures	70
CHAPTER 6	EVENTS SETTINGS	71
6.1	BASIC EVENT CONFIGURATION	71
6.1.1	Configuring Motion Detection	71
6.1.2	Configuring Video Tampering Alarm.....	75
6.1.3	Configuring Alarm Input.....	76
6.1.4	Configuring Alarm Output.....	77
6.1.5	Handling Exception	78
6.2	SMART EVENT CONFIGURATION	78
6.2.1	Detecting Audio Exception	78
6.2.2	Configuring Intrusion Detection.....	80
6.2.3	Configuring Line Crossing Detection	81
6.2.4	Configuring Region Entrance Detection	82
6.2.5	Configuring Region Exiting Detection	83
6.2.6	Configuring Unattended Baggage Detection.....	84
6.2.7	Configuring Object Removal Detection	85
6.3	BEHAVIOR ANALYSIS.....	87
6.3.1	Configuring Overlay & Capture.....	87
6.3.2	Shield Region	88
6.3.3	Rule Configuration	88
6.3.4	Advanced Configuration	92
6.4	FACE CAPTURE.....	93
6.4.1	Overlay & Capture	93
6.4.2	Rule.....	94
6.4.3	Advanced Configuration	95

6.5	PEOPLE DENSITY	97
6.5.1	Rule	97
6.5.2	Data Upload	98
6.5.3	Advanced Configuration	99
6.5.4	Parameters	100
6.6	SMART DISPLAY	100
CHAPTER 7	SYSTEM SETTINGS	101
7.1	BASIC INFORMATION	101
7.1.1	Viewing Basic Information	101
7.1.2	Time Settings	101
7.1.3	Configuring RS-485	103
7.1.4	Configuring DST (Daylight Saving Time)	104
7.1.5	VCA Resource	104
7.1.6	Image Stitching	104
7.1.7	Open Source Software	105
7.2	MAINTENANCE	105
7.2.1	Upgrade & Maintenance	105
7.2.2	Log Searching	107
7.2.3	System Service	108
7.3	SECURITY	108
7.3.1	Configuring Authentication	108
7.3.2	Configuring IP Address Filter	109
7.3.3	Configuring Security Service	110
7.4	USER MANAGEMENT	110
	Online User	111
APPENDIX		112
	APPENDIX 1 SADP SOFTWARE INTRODUCTION	112
	APPENDIX 2 STATICS, INTERFERENCE LIGHTNING AND SURGE PROTECTION	114
	APPENDIX 3 WATERPROOF	117
	APPENDIX 4 BUBBLE MAINTENANCE	118
	APPENDIX 5 RS-485 BUS CONNECTION	119
	APPENDIX 6 24VAC WIRE GAUGE & TRANSMISSION DISTANCE	121
	APPENDIX 7 12VDC WIRE GAUGE & TRANSMISSION DISTANCE	122
	APPENDIX 8 TABLE OF WIRE GAUGE STANDARDS	123
	APPENDIX 9 ALARM IN/OUT CONNECTIONS	124
	APPENDIX 10 CAMERA FUNCTION DESCRIPTION	125

About This Document

This document introduces PanoVu series network camera, including 360° panoramic + PTZ camera, 270° panoramic + PTZ camera, 180° panoramic + PTZ camera, and 360° panoramic camera. It covers how to activate and access to the camera, and operate the camera in the network environment.

Overview of Contents

This document contains the following chapters, sections and appendixes:

- Chapter1 Activating and Accessing to the Camera** provides procedures for setting network environment, activating and accessing the camera by web browsers and client software, and introduces the power-up action.
- Chapter2 Setting Local Parameters and Network** suggests the basic settings, including viewing device local information, configuring saving paths of files, network settings, and other settings.
- Chapter3 Live View** describes how to view video and configure the available settings for the camera via web browser.
- Chapter4 PTZ Control** describes the PTZ function of camera, including preset, patrol, and pattern. It also suggests the PTZ configurations, such as PTZ limits, initial position, and park actions, etc..
- Chapter5 Storage and Playback** introduces how to set the storage, set the recording schedule and capture schedule to trigger the recording and capture by events, and how to view the pictures and play back the saved video files.
- Chapter6 Alarm and Events** explains how to configure the camera to respond to alarm events, and make the events to trigger alarm actions.
- Chapter7 Maintenance** describes how to set the system settings, security settings and user management, including time settings, RS-485 settings, and DST settings, etc.
- Appendix** describes the SADP software, surge protection and details, attention of waterproof measurements and bubble maintenance, RS-485 bus connection details, wire gauge standards and transmission distance, and alarm in/out connections, etc.

Notice

The Camera 1 is the PTZ camera channel, and the Camera 2 and Camera 3 are the panoramic camera channels.

All PTZ functions, including privacy mask, and ROI function are only supported by Camera 1.

Chapter 1 Activating and Accessing to the Camera

1.1 System Requirement

System requirements of web browser accessing are as follows:

Operating System: Microsoft Windows 7 (32 bit/64 bit) and above version

CPU: Intel Pentium IV 3.0 GHz or higher

RAM: 1G or higher

Display: 1024 × 768 resolution or higher

Web Browser: Internet Explorer 11 (Win7/Win8/Win10 32 bit), Internet Explorer 10/9/8 (Win7 32 bit), Mozilla Firefox 30 – 51, and Google Chrome 31 – 44.

1.2 Activating the Camera

1.2.1 Setting the Camera over the LAN

Purpose:

To view and configure the camera via the LAN, you need to connect the camera in the same subnet with your computer, and install the SADP or client software to search and change the IP address of the camera.

Note:

For the detailed introduction of SADP, refer to Appendix 1.

The following figures show the two ways of cable connection of a camera and a computer:

Purpose:

- To test the camera, you can directly connect the camera to the computer with a network cable as shown in Figure 1-1.
- Refer to Figure 1-2 to set the camera over the LAN via a switch or a router.

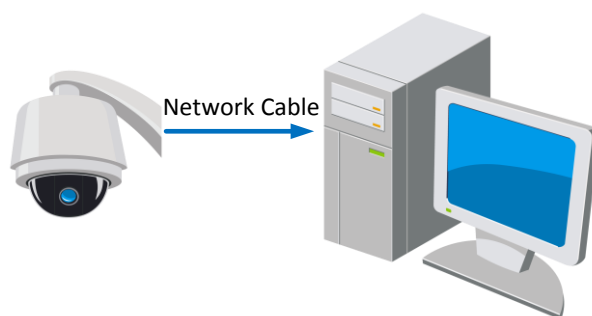


Figure 1-1 Connecting Directly

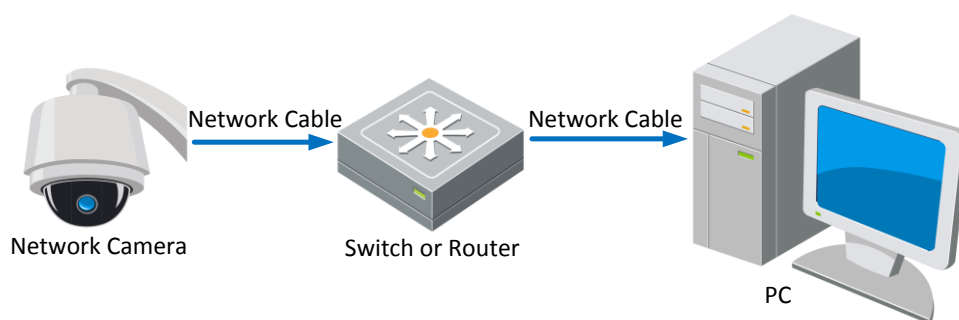


Figure 1-2 Connecting via an Switch or a Router

1.2.2 Activating the Camera

Purpose:

You are required to activate the camera first before you can use the camera.

Activation via web browser, activation via SADP, and activation via client software are supported. In the following sections, activation via web browser and activation via SADP will be taken as examples. You may refer to the user manual of the camera for details of activation via client software.

◆ **Activation via Web Browser**

Steps:

1. Power on the camera, and connect the camera to the network.
2. Input the IP address into the address bar of the web browser, and click **Enter** to enter the activation interface.

Note:

The default IP address of the camera is 192.168.1.64.

Activation	
User Name	admin
Password	
Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.	
Confirm	
OK	

Figure 1-3 Activation Interface (Web Browser)

3. Create a password and input the password into the password field.



STRONG PASSWORD RECOMMENDED— We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Confirm the password.
5. Click **OK** to activate the camera and enter the live view interface.

◆ Activation via SADP Software

SADP software is used for detecting the online device, activating the device, and resetting the password.

Get the SADP software from the supplied disk or the official website, and install the SADP software according to the prompts. Follow the steps to activate the camera.

Steps:

1. Run the SADP software to search the online devices.
2. Check the device status from the device list, and select an inactive device.

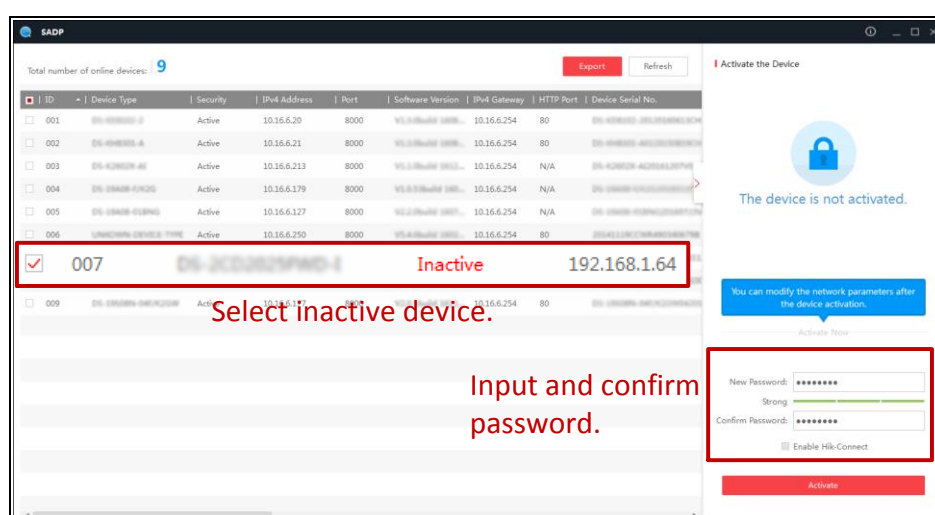


Figure 1-4 SADP Interface

3. Create a password and input the password in the password field, and confirm the password.



STRONG PASSWORD RECOMMENDED— We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **OK** to save the password.

You can check whether the activation is completed on the popup window. If activation failed, make sure that the password meets the requirement and then try again.

5. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the **Enable DHCP** checkbox.

Modify Network Parameters

☐ Enable DHCP

Device Serial No.: XX-XXXXXXXX-XXXXXXXXXXXXXXXX

IP Address: 192.168.1.64

Port: 8000

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Security Verification

Admin Password:

Modify

[Forgot Password](#)

Figure 1-5 Modify the IP Address

6. Input the password and click **Save** to activate your IP address modification.

◆ Activation via Client Software

The client software is versatile video management software for multiple kinds of devices. Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the camera.

Steps:

1. Run the client software and the control panel of the software pops up, as shown in the figure below.

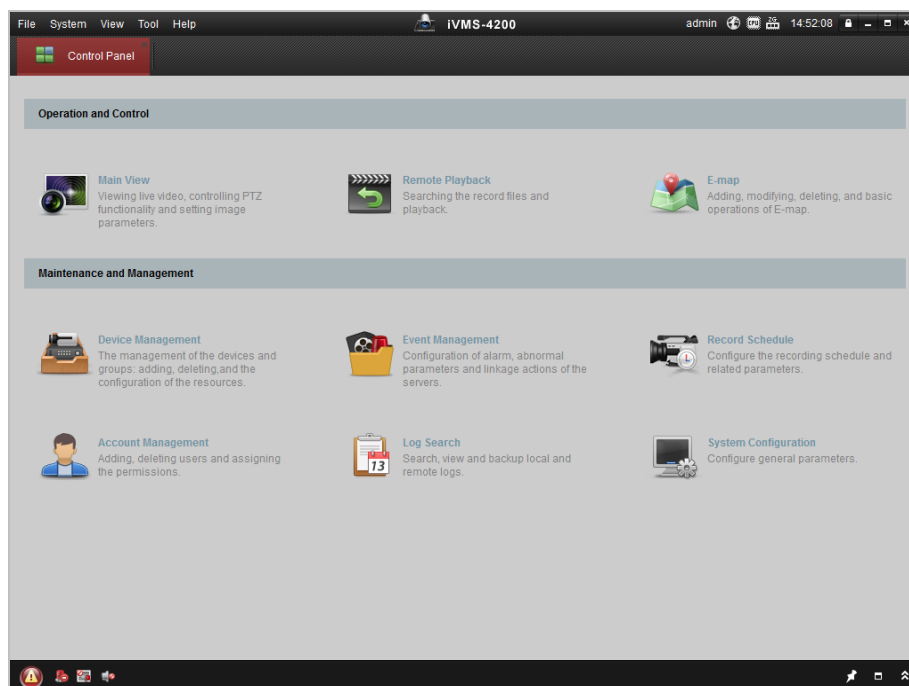


Figure 1-6 Control Panel

- Click **Device Management** to enter the Device Management interface, as shown in the figure below.

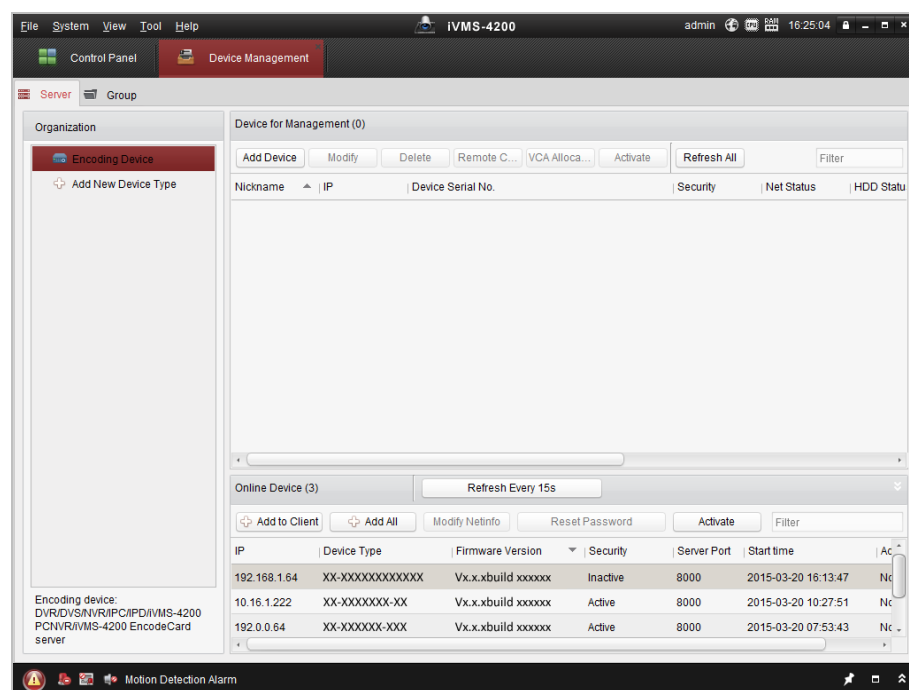


Figure 1-7 Device Management Interface

- Check the device status from the device list, and select an inactive device.
- Click **Activate** to pop up the Activation interface.
- Create a password and input the password in the password field, and confirm the password.



STRONG PASSWORD RECOMMENDED— We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Figure 1-8 Activation Interface

6. Click **OK** to start activation.
7. Click **Modify Netinfo** to pop up the Network Parameter Modification interface, as shown in the figure below.

Figure 1-9 Modifying the Network Parameters

8. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the **Enable DHCP** checkbox.
9. Input the password to activate your IP address modification.

1.3 Setting the Camera over the WAN (Optional)

Purpose:

This section explains how to connect the camera to the WAN with a static IP or a dynamic IP.

1.3.1 Static IP Connection

Before you start:

Apply a static IP from an ISP (Internet Service Provider). With the static IP address, you can connect the camera via a router or connect it to the WAN directly.

◆ **Connecting the camera via a router**

Steps:

1. Connect the camera to the router.
2. Assign a LAN IP address, the subnet mask and the gateway. Refer to **Section 1.2 Activating the Camera** for detailed IP address configuration of the camera.
3. Save the static IP in the router.
4. Set port mapping, E.g., 80, 8000 and 554 ports. The steps for port mapping vary depending on different routers. Call the router manufacturer for assistance with port mapping.

Note:

Refer to Appendix 2 for detailed information about port mapping.

5. Visit the camera through a web browser or the client software over the internet.

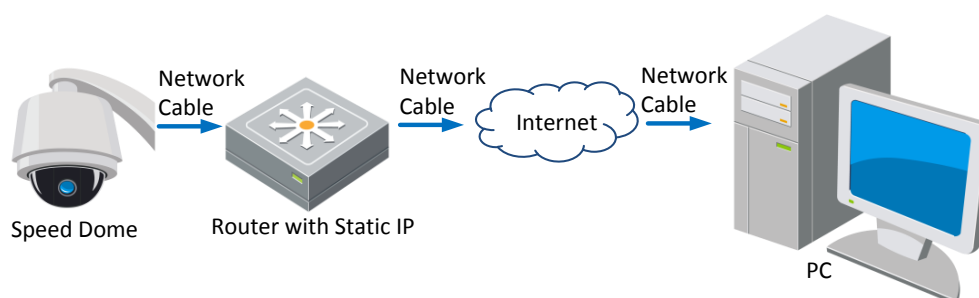


Figure 1-10 Accessing the Camera through Router with Static IP

◆ **Connecting the camera with static IP directly**

You can also save the static IP in the camera and directly connect it to the internet without using a router. Refer to **Section 1.2 Activating the Camera** for detailed IP address configuration of the camera.

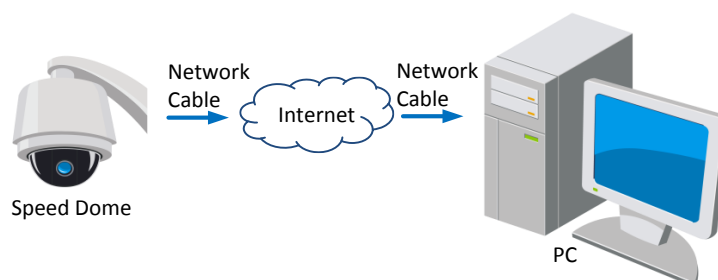


Figure 1-11 Accessing the Camera with Static IP Directly

1.3.2 Dynamic IP Connection

Before you start:

Apply a dynamic IP from an ISP. With the dynamic IP address, you can connect the camera to a modem or a router.

◆ Connecting the camera via a router

Steps:

1. Connect the camera to the router.
2. In the camera, assign a LAN IP address, the subnet mask and the gateway. Refer to **Section 1.2 Activating the Camera** for detailed LAN configuration.
3. In the router, set the PPPoE user name, password and confirm the password.



- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product.*
 - *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*
4. Set port mapping. E.g. 80, 8000 and 554 ports. The steps for port mapping vary depending on different routers. Call the router manufacturer for assistance with port mapping.

Note:

Refer to Appendix 2 for detailed information about port mapping.

5. Apply a domain name from a domain name provider.
6. Configure the DDNS settings in the setting interface of the router.
7. Visit the camera via the applied domain name.

◆ Connecting the camera via a modem

Purpose:

This camera supports the PPPoE auto dial-up function. The camera gets a public IP address by ADSL dial-up after the camera is connected to a modem. You need to configure the PPPoE parameters of the camera. Refer to **Section 2.2.1 Basic Settings - Configuring PPPoE Settings** for detailed configuration.

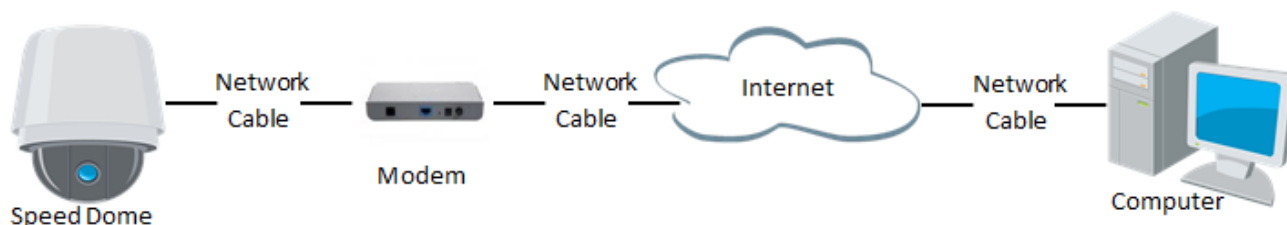


Figure 1-12 Accessing the Camera with Dynamic IP

Note:

The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (E.g. DynDns.com). Follow the steps below for normal domain name resolution and private domain name resolution to solve the problem.

◆ Normal Domain Name Resolution

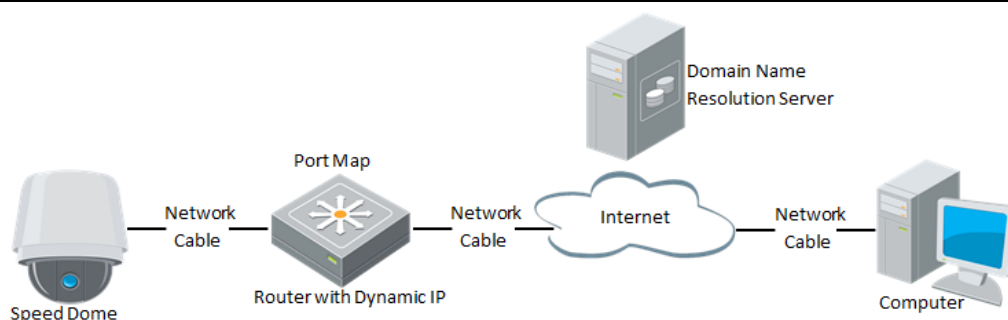


Figure 1-13 Normal Domain Name Resolution

Steps:

1. Apply a domain name from a domain name provider.
2. Configure the DDNS settings in the **DDNS Settings** interface of the camera. Refer to **Section 2.2.1 Basic Settings - Configuring DDNS Settings** for detailed configuration.
3. Visit the camera via the applied domain name.

1.4 Accessing to the Camera

1.4.1 Accessing by Web Browsers

Steps:

1. Open the web browser.
2. In the address field, input the IP address of the camera, e.g., 192.168.1.64 and click **Enter** to enter the login interface.
3. If you activate the camera for the first time using, refer to the **Section 1.2 Activating the Camera**.
4. Select English as the interface language on the top-right of login interface.
5. Input the user name and password and click **Login**.

The admin user should configure the device accounts and user/operator permissions properly. Delete the unnecessary accounts and user/operator permissions.

Note:

The device IP address gets locked if the admin user performs 7 failed password attempts (5 attempts for the user/operator).



Figure 1-14 Login Interface

1.4.2 Accessing by Client Software

The product CD contains the client software. You can view the live video and manage the camera with the client software.

Follow the installation prompts to install the client software and. The configuration interface and live view interface of client software are shown below.

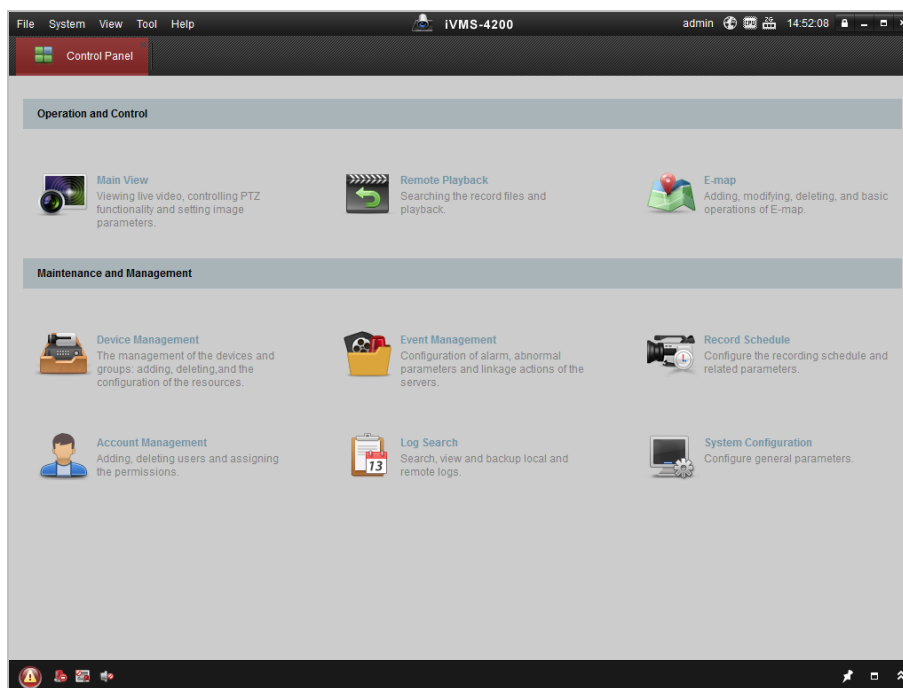


Figure 1-15 iVMS-4200 Control Panel

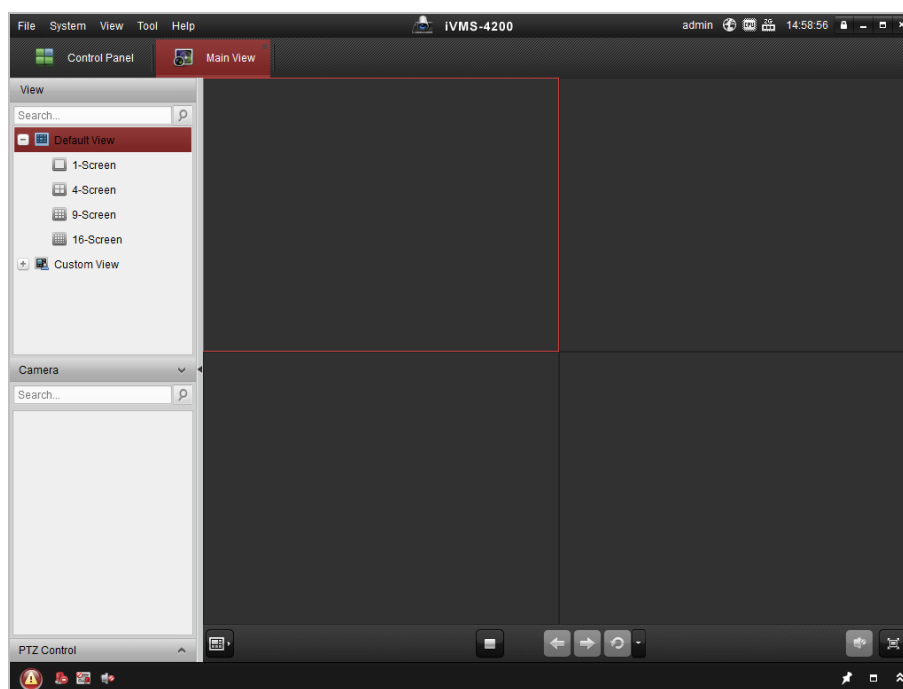


Figure 1-16 iVMS-4200 Live View Interface

Notes:

- If you use third party VMS software, contact technical support of our branch for camera firmware.
- For detailed information about client software of our company, refer to the user manual of the software. This manual mainly introduces accessing to the camera by web browser.

1.5 Power-up Action

After the power is applied, the camera will perform self-test actions. It begins with lens actions and then pan and tilt movement. After the power-up self-test actions, the information shown in Figure 1-17 will be displayed on screen for 40 seconds.

The system information displayed on the screen includes the camera model, address, protocol, version and other information. The COMMUNICATION refers to the baud rate, parity, data bit and stop bit of the camera. e.g., “2400, N, 8, 1” indicates the camera is configured with the baud rate of 2400, no parity, 8 data bits and 1 stop bit.

Model	XX-XXXXXX-X
Address	0
Communication	0000,0,0,0
Software Version	Vx.x.x
Camera Version	Vx.xx
Language	English

Figure 1-17 Power-up Information

Chapter 2 Setting Local Parameters and Network

2.1 Configuring Local Parameters

Note:

The local configuration refers to the parameters of the live view and other operations using the web browser.

Steps:

1. Enter the Local configuration interface:

Configuration > Local

2. Configure the following settings:

- ◆ **Live View Parameters:** Set the protocol type, play performance, rules, and image format.

Live View Parameters				
Protocol	☒ TCP	☐ UDP	☐ MULTICAST	☐ HTTP
Play Performance	☐ Shortest Delay	☒ Balanced	☐ Fluent	
Rules	☐ Enable	☒ Disable		
Display POS Information	☐ Enable	☒ Disable		
Auto Start Live View	☐ Yes	☒ No		
Image Format	☒ JPEG	☐ BMP		

Figure 2-1 Live View Parameters

- **Protocol:** TCP, UDP, MULTICAST and HTTP are selectable.

TCP: Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected.

UDP: Provides real-time audio and video streams.

MULTICAST: It's recommended to select the protocol type to Multicast when using the Multicast function. For other information about Multicast, refer to **Section 2.2.1 Basic Settings - Configuring TCP/IP Settings**.

HTTP: Allows the same quality as of TCP without setting specific ports for streaming under some network environments.

- **Play Performance:** Set the live view performance to Shortest Delay, Balanced or Fluent.

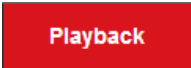
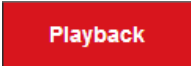
- **Rules:** You can enable or disable the rules of dynamic analysis for events here.

- **Display POS Information:** Enable the function, feature information of the detected target is dynamically displayed near the target in the live image.

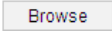
- **Auto Start Live View:** Select **Yes**, then live view is automatically played every time you enter live view interface. Otherwise, you have to click  near live view window to start live view.

- **Image Format:** The captured pictures can be saved in different format. JPEG and BMP are available.

- ◆ **Record File Settings:** Set the saving path of the video files.

- **Record File Size:** Select the packed size of manually recorded and downloaded video files. The size can be set to 256M, 512M or 1G.
- **Save record files to:** Set the saving path for the manually recorded video files.
- **Save downloaded files to:** Set the saving path for the downloaded video files in  interface.
- ◆ **Picture and Clip Settings:** Set the saving paths of the captured pictures and clipped video files.
 - **Save snapshots in live view to:** Set the saving path of the manually captured pictures in  interface.
 - **Save snapshots when playback to:** Set the saving path of the captured pictures in  interface.
 - **Save clips to:** Set the saving path of the clipped video files in  interface.

Note:

You can click  to change the directory for saving video files, clips and pictures.

3. Click  to save the settings.

2.2 Configuring Network Settings

2.2.1 Basic Settings

Configuring TCP/IP Settings

Purpose:

TCP/IP settings must be properly configured before you operate the camera over network. IPv4 and IPv6 are both supported.

Steps:

1. Enter TCP/IP settings interface:
Configuration > Network > Basic Settings > TCP/IP

Figure 2-2 TCP/IP Settings

- Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, MTU settings and Multicast Address.
- (Optional) Check the **Enable Multicast Discovery** checkbox, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.
- Configure the DNS server. Input the preferred DNS server, and alternate DNS server.
- Click  Save to save the above settings.

Notes:

- The valid value range of MTU is 1280 ~ 1500.
- The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before utilizing this function, you have to enable the Multicast function of your router.
- Reboot the device before the settings take effect.

Configuring DDNS Settings**Purpose:**

If your camera is set to use PPPoE as its default network connection, you can use the Dynamic DNS (DDNS) for network access.

Before you start:

Registration on the DDNS server is required before configuring the DDNS settings of the camera.



- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (Using a minimum of 8 characters, including at least three of

the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product.

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Steps:

1. Enter the DDNS settings interface:

Configuration > Network > Basic Settings > DDNS

Figure 2-3 DDNS Settings

2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Two DDNS types are selectable: DynDNS and NO-IP.

● DynDNS:

Steps:

- (1) Input **Server Address** of DynDNS (e.g. members.dyndns.org).
- (2) In the **Domain** text field, input the domain name obtained from the DynDNS website.
- (3) Input the **Port** of DynDNS server.
- (4) Input the **User Name** and **Password** registered on the DynDNS website.

- (5) Click  Save to save the settings.

Figure 2-4 DynDNS Settings

● NO-IP:

Steps:

- (1) Input **Server Address** of NO-IP.
- (2) In the **Domain** text field, input the domain name obtained from the NO-IP website.
- (3) Input the **Port** of NO-IP server.
- (4) Input the **User Name** and **Password** registered on the NO-IP website.

- (5) Click  Save to save the settings.

Configuring PPPoE Settings

Purpose:

If you have no router but only a modem, you can use Point-to-Point Protocol over Ethernet (PPPoE) function.

Steps:

1. Enter the PPPoE settings interface:

Configuration > Network > Basic Settings > PPPoE



Figure 2-5 PPPoE Settings

2. Check the **Enable PPPoE** checkbox to enable this feature.
3. Input **User Name**, **Password**, and **Confirm** password for PPPoE access.

Note:

The User Name and Password should be assigned by your ISP.



- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

4. Click  to save and exit the interface.

Configuring Port Settings

Purpose:

You can set the port No. of the camera, e.g., HTTP port, RTSP port and HTTPS port.

Steps:

1. Enter the Port settings interface:

Configuration > Network > Basic Settings > Port

TCP/IP	DDNS	PPPoE	Port	NAT	Multicast
			HTTP Port	80	
			RTSP Port	554	
			HTTPS Port	443	
			Server Port	8000	
			Enhanced SDK Service P...	8443	
			WebSocket Port	7681	
			WebSockets Port	7682	

Figure 2-6 Port Settings

2. Set the HTTP port, RTSP port and port of the camera.

- **HTTP Port:** The default port number is 80.
- **RTSP Port:** The default port number is 554.
- **HTTPS Port:** The default port number is 443.
- **Server Port:** The default port number is 8000.

Note:

When you use client software to visit the camera and you have changed the server port number, you have to input the correct server port number in login interface to access to the camera.

- **Enhanced SDK Service Port:** The default server port number is 8443, and it can be changed to any port number ranges from 2000 to 65535.
- **WebSocket Port:** The default port number is 7681.
- **WebSockets Port:** The default server port number is 7682.

Note:

WebSocket and WebSockets protocol are used for plug-in free live view. For detailed information, see **Network Service** in **Section 2.2.2 Advanced Settings**.

3. Click  to save the settings.

Configuring NAT (Network Address Translation) Settings

Purpose:

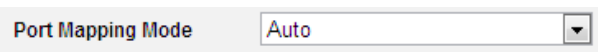
Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the house and corporate environments.

With the function enabled, you don't need to configure the port mapping for each port, and the camera is connected to the Wide Area Network via the router.

Steps:

1. Enter the NAT settings interface by
Configuration > Network > Basic Settings > NAT
2. Check the ☒ **Enable UPnP™** checkbox to enable the UPnP™ function.
3. Set the port mapping mode:

To port mapping with the default port numbers:

Choose  **Auto**

To port mapping with the customized port numbers:

Choose **Port Mapping Mode** Manual

And you can customize the value of the port No. by yourself.

☒ Enable UPnP™

Nickname 

Port Mapping Mode Auto

Port Type	External Port	External IP Address	Internal Port	Status
HTTP	80	0.0.0.0	80	Valid
RTSP	554	0.0.0.0	554	Valid
Server Port	8000	0.0.0.0	8000	Valid

Figure 2-7 Configure the Port No.

4. Click  to save the settings.

2.2.2 Advanced Settings

Configuring SNMP Settings

Purpose:

You can use SNMP to get camera status and parameters related information.

Before you start:

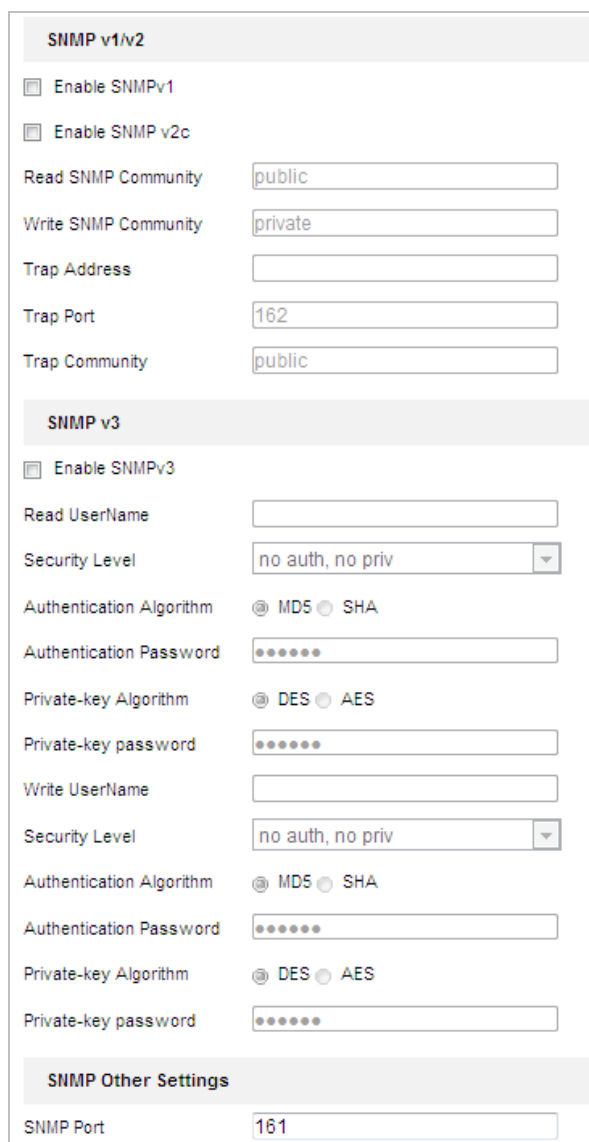
Before setting the SNMP, use the SNMP software and manage to receive the camera information via SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center.

Note:

The SNMP version you select should be the same as that of the SNMP software.

Steps:

1. Enter the SNMP settings interface:
Configuration > Network > Advanced Settings > SNMP



The image shows a web-based configuration interface for SNMP settings, divided into three main sections: SNMP v1/v2, SNMP v3, and SNMP Other Settings.

SNMP v1/v2

- ☒ Enable SNMPv1
- ☒ Enable SNMP v2c
- Read SNMP Community: public
- Write SNMP Community: private
- Trap Address: (empty field)
- Trap Port: 162
- Trap Community: public

SNMP v3

- ☒ Enable SNMPv3
- Read UserName: (empty field)
- Security Level: no auth, no priv (dropdown menu)
- Authentication Algorithm: ☒ MD5 ☐ SHA
- Authentication Password: (masked field with 6 dots)
- Private-key Algorithm: ☒ DES ☐ AES
- Private-key password: (masked field with 6 dots)
- Write UserName: (empty field)
- Security Level: no auth, no priv (dropdown menu)
- Authentication Algorithm: ☒ MD5 ☐ SHA
- Authentication Password: (masked field with 6 dots)
- Private-key Algorithm: ☒ DES ☐ AES
- Private-key password: (masked field with 6 dots)

SNMP Other Settings

- SNMP Port: 161

Figure 2-8 SNMP Settings

- Check the corresponding version checkbox (**Enable SNMP v1**, **Enable SNMP v2c**, **Enable SNMP v3**) to enable the feature.
- Configure the SNMP settings.

Note:

The configuration of the SNMP software should be the same as the settings you configure here.

- Click  to save and finish the settings.

Configuring FTP Settings

Purpose:

You can configure the FTP server related information to enable the uploading of the captured pictures to the FTP server. The captured pictures can be triggered by events or a timing snapshot task.

Steps:

- Enter the FTP settings interface:
Configuration > Network > Advanced Settings > FTP

Figure 2-9 FTP Settings

- Input the FTP address and port.

Note:

The server address supports both the domain name and IP address formats.

- Configure the FTP settings. The user name and password are required for the FTP server login.



- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product.
 - Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- Set the directory structure and picture filing interval.

Directory: In the **Directory Structure** field, you can select the root directory, parent directory and child directory. When the parent directory is selected, you have the option to use the Device Name, Device Number or Device IP for the name of the directory; and when the Child Directory is selected, you can use the Camera Name or Camera No. as the name of the directory.

Figure 2-10 Parent Directory

Figure 2-11 Child Directory

Picture Filing Interval: For better picture management, you can set the picture filing interval from 1 day to 30 days. Pictures captured in the same time interval will be saved in one folder named after the beginning date and ending date of the time interval.

Picture Name: Set the naming rule for captured picture files. You can choose **Default** in the drop-down list to use the default rule, that is,

IP address_channel number_capture time_event type.jpg
(e.g., 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg)

Or you can customize it by adding a **Custom Prefix** to the default naming rule.

5. Check the Upload Picture checkbox to enable the function.

Upload Picture: To enable uploading the captured picture to the FTP server.

Anonymous Access to the FTP Server (in which case the user name and password won't be required.): Check the **Anonymous** checkbox to enable the anonymous access to the FTP server.

Note: The anonymous access function must be supported by the FTP server.

6. Save the settings.

Configuring Email Settings

Purpose:

The system can be configured to send an Email notification to all designated receivers if an alarm event is detected, e.g., motion detection event, video tampering, etc.

Before you start:

Configure the DNS Server settings under **Configuration > Network > Basic Settings > TCP/IP** before using the Email function.

Steps:

1. Enter the Email settings interface:

Configuration > Network > Advanced Settings > Email

Sender	
Sender's Address	
SMTP Server	
SMTP Port	25
E-mail Encryption	None
☐ Authentication	
User Name	
Password	
Confirm	

Receiver			
No.	Receiver	Receiver's Address	Test
1			Test
2			
3			

Figure 2-12 Email Settings

2. Configure the following settings:

Sender: The name of the email sender.

Sender's Address: The email address of the sender.

SMTP Server: The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

SMTP Port: The SMTP port. The default TCP/IP port for SMTP is 25.

E-mail Encryption: Email encryption can be selected among None, SSL, and TLS. When you select SSL or TLS and disable STARTTLS, e-mails will be sent after encrypted by SSL or TLS. The SMTP port should be set as 465 for this encryption method. When you select SSL or TLS and enable STARTTLS, emails will be sent after encrypted by STARTTLS, and the SMTP port should be set as 25.

Note:

If you want to use STARTTLS, make sure that the protocol is supported by your e-mail server. If you check the Enable STARTTLS checkbox when the protocol is not supported by your e-mail sever, your e-mail will not be encrypted.

Authentication (optional): If your email server requires authentication, check this checkbox to use authentication to log in to this server and input the login user name and password.



- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Receiver: Input the receiver to which the email is sent.

Receiver's Address: The email address of user to be notified.

Note:

You can click  to check whether the setting is invalid after the required parameters are configured.

3. Click  to save the settings.

Configuring HTTPS Settings

Purpose:

HTTPS provides authentication of the web site and associated web server that one is communicating with, which protects against Man-in-the-middle attacks. Perform the following steps to set the port number of https.

Example:

If you set the port number as 443 and the IP address is 192.168.1.64, you may access the device by inputting `https://192.168.1.64:443` via the web browser.

Note:

- For the camera that supports plug-in free live view, when you use HTTPS to visit the camera, you should enable **Websockets** for live view. Go to **Configuration > Network > Advanced Settings > Network Service**.
- HTTPS is enabled by default. The camera creates an unsigned certificate automatically. When you visit the camera via HTTPS, the web browser will send a notification about the certificate issue. Install a signed-certificate to the camera to cancel the notification.

Steps:

1. Enter the HTTPS settings interface.
Configuration > Network > Advanced Settings > HTTPS
2. Create the self-signed certificate or authorized certificate.

Figure 2-13 Create Certificate

OPTION 1: Create the self-signed certificate

- 1) Select **Create Self-signed Certificate**.
- 2) Click **Create** to create the following dialog box.

Figure 2-14 Create Self-signed Certificate

- 3) Input the country, host name/IP, validity and other information.
- 4) Click **OK** to save the settings.

OPTION 2: Start the installation when signed certificate is available.

- 1) Select **Signed certificate is available, Start the installation directly**.
- 2) Click **Browse** to upload the available certificate.
- 3) Click **Install** button to install the certificate.
- 4) Click **OK** to save the settings.

OPTION 3: Create certificate request first and continue the installation.

- 1) Select **Create certificate request first and continue the installation**.
 - 2) Click **Create** to create the certificate request, and fulfill the required information.
 - 3) Download the certificate request and submit it to the trusted certificate authority for signature.
 - 4) After receiving the signed valid certificate, import the certificate to the device.
 - 5) Click **OK** to save the settings.
3. There will be the certificate information after you successfully create and install the certificate.

Figure 2-15 Installed Certificate Property

Note:

You can click configure the HTTPS port No. on your demand; refer to **Section 2.2.1 Basic Settings - Configuring Port Settings** for details.

4. Check the **Enable HTTPS** checkbox and click **Save**.

Configuring QoS Settings

Purpose:

QoS (Quality of Service) can help solve the network delay and network congestion by configuring the priority of data sending.

Steps:

1. Enter the QoS settings interface:

Configuration > Network > Advanced Settings > QoS

Video/Audio DSCP	0
Event/Alarm DSCP	0
Management DSCP	0

Figure 2-16 QoS Settings

2. Configure the QoS settings, including video/audio DSCP, event/alarm DSCP and Management DSCP. The valid DSCP value ranges from 0 to 63. The DSCP value is bigger, the priority is higher.

3. Click  to save the settings.

Notes:

- Make sure that you enable the QoS function of your network device (such as a router).
- Reboot the device before the settings take effect.

Configuring 802.1X Settings

Purpose:

The camera supports IEEE 802.1X standard.

IEEE 802.1X is a port-based network access control. It enhances the security level of the LAN. When devices connect to this network with IEEE 802.1X standard, the authentication is needed. If the authentication fails, the devices don't connect to the network.

The protected LAN with 802.1X standard is shown as follows:

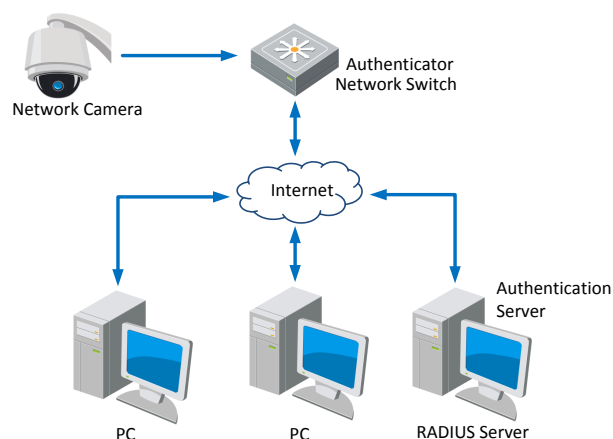


Figure 2-17 Protected LAN

- Before connecting the network camera to the protected LAN, apply a digital certificate from a Certificate Authority.
- The network camera requests access to the protected LAN via the authenticator (a switch).
- The switch forwards the identity and password to the authentication server (RADIUS server).
- The switch forwards the certificate of authentication server to the network camera.
- If all the information is validated, the switch allows the network access to the protected network.



- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Steps:

1. Connect the network camera to your PC directly with a network cable.
2. Enter the 802.1X settings interface:

Configuration > Network > Advanced Settings > 802.1X

Figure 2-18 802.1X Settings

3. Check the **Enable IEEE 802.1X** checkbox to enable it.
4. Configure the 802.1X settings, including user name and password.

Note:

The EAP-MD5 version must be identical with that of the router or the switch.

5. Click  to finish the settings.

Note:

The camera reboots when you save the settings.

6. After the configuration, connect the camera to the protected network.

Integration Protocol

If you need to access to the camera through the third party platform, you can enable CGI function. And if you need to access to the device through ONVIF protocol, you can configure ONVIF user in this interface. Refer to ONVIF standard for detailed configuration rules.

Note:

Supported protocols may be different among camera models.

- CGI

Check the **Enable ***CGI** checkbox and then select the authentication from the drop-down list. Then you can access to the camera through the third party platform.

- **ONVIF**

Steps:

1. Check the **Enable ONVIF** checkbox to enable the function.
2. Click **Add** to add a new ONVIF user. Set the user name and password, and confirm the password. You can set the user as media user, operator, and administrator.
3. Click **Modify** to modify the information of the added ONVIF user.
4. Click **Delete** to delete the selected ONVIF user.
5. Save the settings.

Note:

User settings of ONVIF are cleared when you restore the camera.

Network Service

Purpose:

You can control the ON/OFF status of certain protocol that the camera supports.

Notes:

Supported services vary according to camera models.

Keep unused function OFF for security concern.

- **WebSocket** or **WebSockets** protocol are used for plug-in-free live view.
When you use Google Chrome 57 and its above version or Mozilla Firefox 52 and its above version to visit your camera, you should enable WebSocket or Websokets protocol. Otherwise, live view function is not usable.
If the camera uses HTTP, enable **WebSocket**.
If the camera uses HTTPS, enable **WebSockets**.
- **SDK Service** and **Enhanced SDK Service**
If you want to add the device to the client software, you should enable SDK Service or Enhanced SDK Service.
SDK Service: SDK protocol is used.
Enhanced SDK Service: SDK over TLS protocol is used. Communication between the device and the client software is secured by using TLS (Transport Layer Security) protocol.
- **TLS (Transport Layer Security)**
The device offers TLS 1.1 and TLS 1.2. Enable one or more protocol versions according to your need.

Chapter 3 Live View

3.1 Install the Plug-in

Install the plug-in before viewing the live video and operating the camera. Follow the installation prompts to install the plug-in.

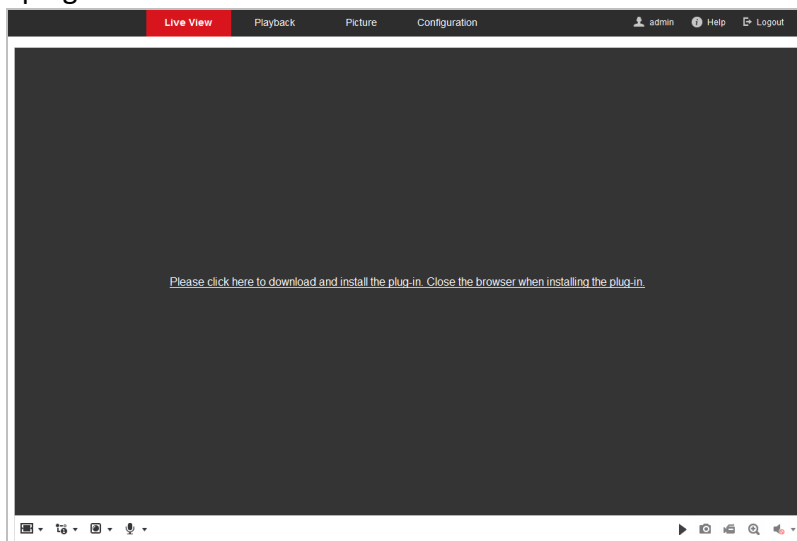


Figure 3-1 Download and Install Plug-in

Notes:

- You may have to close the web browser to install the plug-in. Reopen the web browser and log in again after installing the plug-in.
- To select the plug-in type, you can click  on live view interface. For detailed information, refer to **Section 3.2.2 Live View Operation**.

3.2 Live View Page

3.2.1 Descriptions of the live view page:

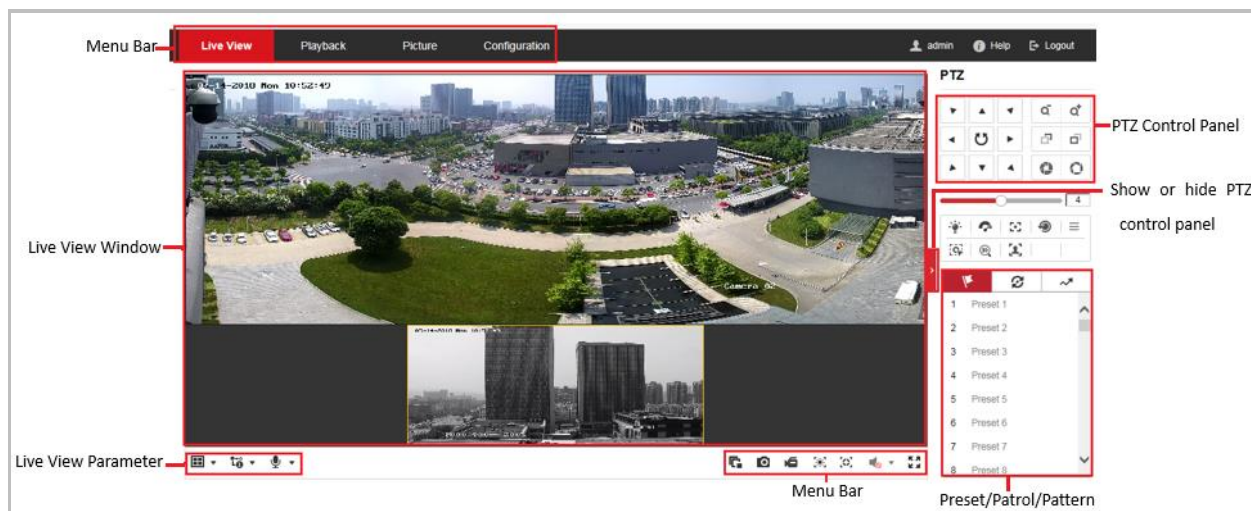


Figure 3-2 Live View Page

Menu Bar:

Click each tab to enter Live View, Playback, Picture, and Configuration page respectively.

Click to display the help file of the camera.

Click to logout the system.

Live View Window:

Display the live video.

Toolbar:

Operations on the live view page, e.g., live view, capture, record, audio on/off, regional exposure, regional focus, etc.

PTZ Control:

Panning, tilting, focusing and zooming actions of the camera. The lighter, wiper, one-touch focus and lens initialization control.

Preset/patrol/pattern:

Set and call the preset/patrol/pattern for the camera.

Live View Parameters:

Configure the window division, image size, stream type, plug-in type, and two-way audio of the live video.

3.2.2 Live View Operation

Purpose:

The live video page allows you to view live video, capture images, realize PTZ control, set/call presets and configure video parameters.

Log in the camera to enter the live view page, or you can click **Live View** on the menu bar of the main page to enter the live view page.

Starting Live View

Click  on the toolbar to start the live view of all channels of the network camera. Live view page of panoramic + PTZ camera and panoramic camera are different as shown below.

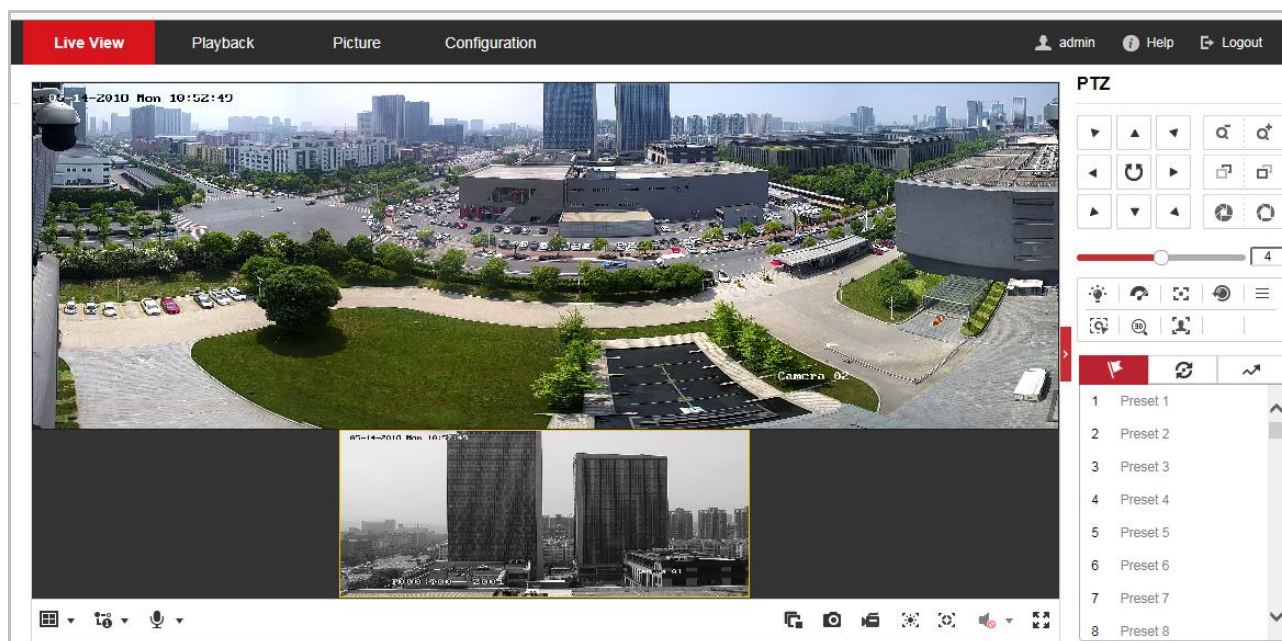


Figure 3-3 Start Live View (Panoramic + PTZ Camera)

Descriptions of Icons on Toolbar and Live View Interface are listed below:

Live View  Click  to start all live views and the icon turns into . Click the icon again to stop all live views.

Full-screen  Double-click  on the live video to switch the current live view into full-screen or return to normal mode from the full-screen.

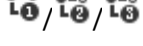
Record/Capture  Click  to manual capture the picture.



Click  to start manual recording and the icon turns into . Click the icon again to stop recording.

Note: Before perform manual recording and manual capture, configure the saving path of files referring to **Section 2.1**.

Window Division  For 360° panoramic + PTZ camera, click  to select from  and display live video in triple-row/double-row/ $1 \times 1/2 \times 2$ /PIP (Picture in Picture) window size.

Stream Type  Click  to select from  and display live video with the main/sub/third stream. The main stream is with a relatively high resolution and needs much bandwidth. The sub-stream is with a low resolution and needs less bandwidth. The resolution of third stream is between that of main

stream and sub stream. The default setting of stream type is .

Plug-in Switch	 / 	Click  to select between  and  and play the live video via player Webcomponents or Quick Time. The live video is played via webcomponents by default, and other types of players are supported for the browser, such as MJPEG, and VLC. You are required to download and install the player to play the live video.
Audio	 / 	Volume Click  to display the . Drag the slider to adjust the volume.
	 / 	Two-way Audio Click  and it displays . Click  to enable two-way audio and the icon turns into . Click the icon again to stop two-way audio. Note: Before enabling the two-way audio or recording with audio functions, set the Stream Type to Video & Audio referring to Section 3.4.1 Configuring Video Settings.
Digital Zoom	 / 	Click  to enable digital zoom function and the icon turns into  . Then scroll the mouse wheel up/down to zoom in/out the live view image.
Regional Exposure	 / 	Click  on the toolbar to enter the regional exposure operation mode and the icon turns into  . Then drag the mouse to draw a rectangle on the image as the desired exposure region.
Regional Focus	 / 	Click  on the toolbar to enter the regional focus operation mode and the icon turns into  . Then drag the mouse to draw a rectangle on the image as the desired focus region.

PTZ Control Panel

On the live view page, click  to show the PTZ control panel or click  to hide it.

Descriptions of Icons on PTZ Control Panel are listed below:

PTZ Control		Hold the direction buttons to control the pan/tilt movements. Click  and the camera keeps panning, the icon turns into . Click the icon again to stop the camera.
Zoom		Click  , the lens zooms in, click  , and the lens zooms out.

Focus		Click  , the lens focus far and the items far away gets clear. Click  , the lens focus near and the items nearby gets clear.
Iris		When the image is too dark, click  to open the iris. When the image is too bright, click  to close the iris.
Adjust Speed		Adjust speed of pan/tilt movements.
Preset		Refer to 4.1.1 for detailed information of setting preset.
Patrol		Refer to 4.1.2 for detailed information of setting patrol.
Pattern		Refer to 4.1.3 for detailed information of setting pattern.

Note:

PTZ functions, including PTZ control, preset, patrol, and pattern are only supported by camera 1.

Auxiliary Functions

The auxiliary functions include light, wiper, auxiliary focus, lens initialization, manual tracking, 3D positioning, one-touch patrol, and one-touch park.

The Auxiliary functions panel is shown in the figure below:



Figure 3-4 Auxiliary Functions

Descriptions of Icons on PTZ Control Panel are listed below:

Light Supplement		Click  to enable/disable the light supplement of the camera. This function is reserved.
Wiper		Click  to move the wiper once.
Auxiliary Focus		The auxiliary focus function is reserved.
Manual Tracking		Before you start: Enter the Smart Tracking settings interface and enable smart tracking first. Configuration > PTZ > Smart Tracking Steps: 1. Click  on the toolbar of live view interface. 2. Click a moving object in the live video. The camera will track the object automatically.
3D Positioning		Steps: 1. Click  on the toolbar of live view interface. 2. Operate the 3D positioning function: ● Left click a position of the live video. The corresponding position will be moved to the center of the live video.

- Hold down the left mouse button and drag the mouse to the lower right on the live video. The corresponding position will be moved to the center of the live video and zoomed in.
- Hold down the left mouse button and drag the mouse to the upper left on the live video. The corresponding position will be moved to the center of the live video and zoomed out.

Note:

When you perform 3D positioning on Camera 2 or Camera 3, the Camera 1 will move to the corresponding position.

Lens Initialization

Click  and the lens operates the movements for initialization.

Face Capture**Steps:**

1. Click  to start manual face capture.
2. Frame the target face in PTZ camera channel by left-click and drag to draw a frame.
3. Click the icon again to stop manual face capture.

Note:

To use manual face capture, you should configure **Face Capture** function first. Go to **Configuration > Face Capture**. The function is only available for certain camera models.

3.3 Configuring Image Settings

3.3.1 Configuring Display Settings

Purpose:

You can set the image related parameters of the camera, including brightness, contrast, saturation, sharpness, etc.

Notes:

- The parameters in **Display Settings** interface vary depending on different camera models.
- You can double click the live view to enter full screen mode and double click it again to exit.
- Available parameters for PTZ camera channel and panoramic camera channel are different. The following introduction covers all possible parameters you can set in **Display Settings** for this camera series.

Steps:

1. Enter the Display Settings interface:

Configuration > Image > Display Settings

2. For the camera model that has more than one panoramic camera channel, you can set parameters applying to **Multiple Channel** and **Single Channel** separately.

Panoramic Exposure Synchronization: Enable this function to balance exposure panoramic camera channels.

Channel No.: For single channel settings, select a channel to specify its parameters.

Mounting Scenario: Select according to actual mounting environment of the camera to make the configuration more accurate.

3. Set the image parameters of the camera channel.

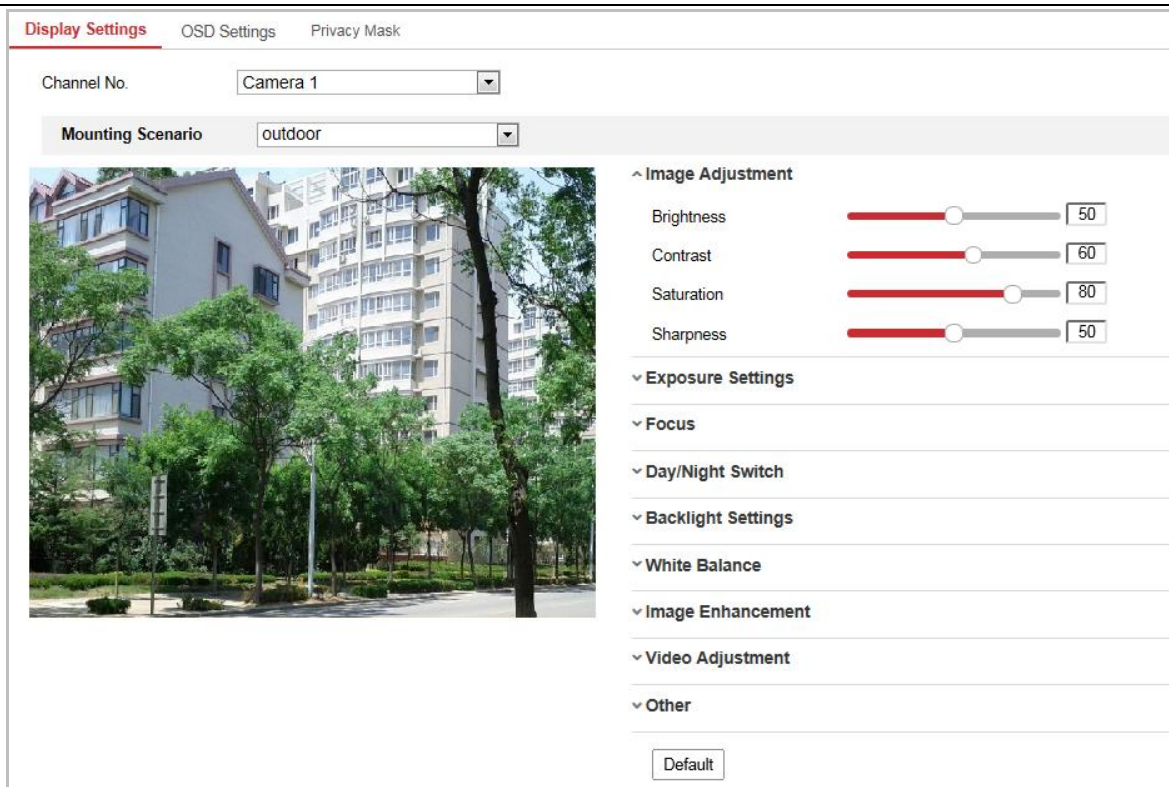


Figure 3-5 Display Settings

Image Adjustment

- **Brightness**

This feature is used to adjust brightness of the image. The value ranges from 0 to 100.

- **Contrast**

This feature enhances the difference in color and light between parts of an image. The value ranges from 0 to 100.

- **Saturation**

This feature is used to adjust color saturation of the image. The value ranges from 0 to 100.

- **Sharpness**

Sharpness function enhances the detail of the image by sharpening the edges in the image. The value ranges from 0 to 100.

Exposure Settings

- **Exposure Mode**

The **Exposure Mode** can be set to **Auto**, **Iris Priority**, **Shutter Priority**, and **Manual**.

- **Auto:**

The iris, shutter and gain values will be adjusted automatically according to the brightness of the environment.

- **Iris Priority:**

The value of iris needs to be adjusted manually. The shutter and gain values will be adjusted automatically according to the brightness of the environment.

Exposure Mode	Iris Priority
Exposure Level	<input type="range"/> 4
Max.Shutter Limit	1/25
Min.Shutter Limit	1/30000
Iris	f1.6
Limit Gain	<input type="range"/> 94
Slow Shutter	OFF

Figure 3-6 Manual Iris

- **Shutter Priority:**

The value of shutter needs to be adjusted manually. The iris and gain values will be adjusted automatically according to the brightness of the environment.

Exposure Mode	Shutter Priority
Exposure Level	<input type="range"/> 4
Max. Iris Limit	<input type="range"/> 100
Min. Iris Limit	<input type="range"/> 0
Shutter	1/25
Limit Gain	<input type="range"/> 94
Slow Shutter	OFF

Figure 3-7 Manual Shutter

- **Manual:**

In **Manual** mode, you can adjust the values of **Gain**, **Shutter**, **Iris** manually.

Note:

This function varies depending on different camera models.

- **Limit Gain**

This feature is used to adjust gain of the image. The value ranges from 0 to 100.

- **Slow Shutter**

This function can be used in underexposure condition. It lengthens the shutter time to ensure full exposure. Select slow shutter level from the dropdown list

Slow Shutter	ON
Slow Shutter Level	Slow Shutter*2

Figure 3-8 Slow Shutter

- **Sensor's Exposure Sync.** (only available for panoramic camera channel)

It is used to balance the exposure within a panoramic camera channel whose image are stitched from four camera sensors.

Focus Settings

- **Focus Mode**

The **Focus Mode** can be set to **Auto**, **Manual**, **Semi-auto**.

- **Auto:**

The camera focuses automatically at any time according to objects in the scene.

- **Semi-auto:**

The camera focuses automatically only once after panning, tilting and zooming.

- **Manual:**

In **Manual** mode, you need to use   on the control panel to focus manually.

- **Min. Focus Distance**

This function is used to limit the minimum focus distance.

Note:

Focus settings applies only to PTZ camera channel.

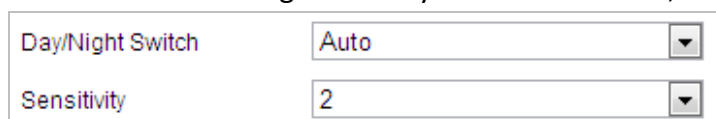
Day/Night Switch

- **Day/Night Switch**

The **Day/Night Switch** mode can be set to **Auto**, **Day**, **Night**, and **Scheduled-Switch**.

- **Auto:**

In **Auto** mode, the day mode and night mode can switch automatically according to the light condition of environment. The switching sensitivity can be set to **Low**, **Normal**, **High**.



Day/Night Switch	Auto
Sensitivity	2

Figure 3-9 Auto Mode Sensitivity

- **Day:**

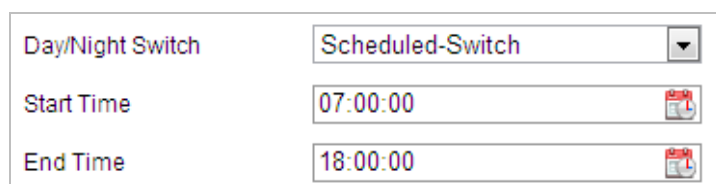
In **Day** mode, the camera displays color image. It is used for normal lighting conditions.

- **Night:**

In **Night** mode, the image is black and white. **Night** mode can increase the sensitivity in low light conditions.

- **Scheduled-Switch**

In **Scheduled-Switch** mode, you can set the time schedule for day mode as shown in Figure 3-10. The rest time out of the schedule is for night mode.



Day/Night Switch	Scheduled-Switch
Start Time	07:00:00
End Time	18:00:00

Figure 3-10 Day Night Schedule

- **Smart Supplement Light**

If the light supplement is on and the image center is overexposure, you can enable this function.

- **IR Light Mode**

IR light mode can be set to **Auto** and **Manual**.

- **Auto:** The brightness of the infrared light will be adjusted automatically. **IR Light Sensitivity** value ranges from 0 to 100. **Trigger Mode** can be set to **Camera** or **Photosensitive**.
- **Manual:** you need to adjust the brightness value of infrared light manually. **Brightness Limit** value ranges from 0 to 100.

Notes:

- This function varies depending on different camera models.
- The IR related functions are supported by the IR camera only.

- For detailed parameters configuration of IR light, you can enter the OSD menu by calling the special preset 95.
- When the **IR Light Mode** is auto, the day/night mode is adjusted automatically according to the IR Light Mode. Manually setting the day/night mode is invalid.
- When the **IR Light Mode** is manual and the **Brightness Limit** is 0, you can set the day/night mode manually.
- When the **IR Light Mode** is manual and the **Brightness Limit** is not 0, the night mode is set as the default mode. Manually setting the day/night mode is invalid.

Backlight Settings

● BLC (Back Light Compensation)

If there's a bright backlight, the subject in front of the backlight appears silhouetted or dark. Enabling **BLC** (back light compensation) function can correct the exposure of the subject. But the backlight environment is washed out to white.

● WDR (Wide Dynamic Range)

The wide dynamic range (WDR) function helps the camera provide clear images even under back light circumstances. When there are both very bright and very dark areas simultaneously in the field of view, WDR balances the brightness level of the whole image and provide clear images with details.

You can enable or disable the WDR function as shown in Figure 3-11. The wide dynamic level ranges from 0 to 100.



Figure 3-11 WDR

Note:

This function varies depending on different camera models.

● HLC

HLC (High Light Compensation) makes the camera identify and suppress the strong light sources that usually flare across a scene. This makes it possible to see the detail of the image that would normally be hidden.

White Balance

The **White Balance** mode can be set to **Auto**, **MWB**, **Outdoor**, **Indoor**, **Fluorescent Lamp**, **Sodium Lamp** and **Auto-Tracking**.

● Auto

In **Auto** mode, the camera retains color balance automatically according to the current color temperature.

● MWB

In **MWB** (Manual White Balance) mode, you can adjust the color temperature manually to meet your own demand as shown in Figure 3-12.

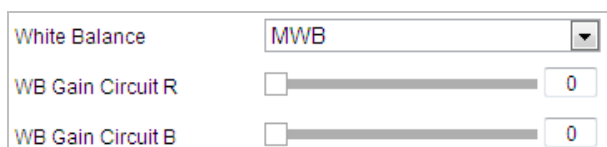


Figure 3-12 Manual White Balance

- **Outdoor**

You can select this mode when the camera is installed in outdoor environment.

- **Indoor**

You can select this mode when the camera is installed in indoor environment.

- **Fluorescent Lamp**

You can select this mode when there are fluorescent lamps installed near the camera.

- **Sodium Lamp**

You can select this mode when there are sodium lamps installed near the camera.

- **Auto-Tracking**

In **Auto-Tracking** mode, white balance is continuously being adjusted in real-time according to the color temperature of the scene illumination.

Image Enhancement

- **Digital Noise Reduction**

The digital noise reduces function processes the noise in the video signal.

You can set **Digital Noise Reduction** function to **Normal** and adjust the **Noise Reduction Level** as shown in Figure 3-13. The level ranges from 0 to 100.

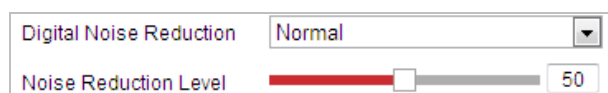


Figure 3-13 Normal Mode

If you are a professional technician, you can set it to Expert Mode then adjust Space DNR Level and Time DNR Level.

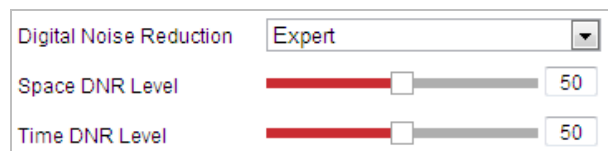


Figure 3-14 Expert Mode

- **Defog Mode**

When there is fog in the image, you can enable this function to get clear image.

- **EIS (Electronic Image Stabilization)**

The live view image would be trembled and dim when the camera is shocked slightly in some monitoring conditions. And the electronic image stabilization (EIS) function is used to overcome this problem to ensure a steady and clear image.

- **OIS (Optical Image Stabilization)**

You can set the OIS (Optical Image Stabilization) to NORMAL, EXPERT, or OFF as you need. In expert mode, you can specify OIS level and OIS Sensitivity.

Video Adjustment

- **Mirror**

If you turn the **MIRROR** function on, the image will be flipped. It is like the image in the mirror. The flip direction can be set to OFF, or CENTER.

- **Video Standard**

You can set the **Video Standard** to 50 Hz (PAL) or 60 Hz (NTSC) according to the video system in your country.

● Capture Mode:

The **Capture Mode** can be selected from the list.

Other

● Lens Initialization

The lens operates the movements for initialization when you check the **Lens Initialization** checkbox.

● Zoom Limit

You can set **Zoom Limit** value to limit the maximum value of zooming. The value can be selected from the list.

Note:

Lens Initialization and **Zoom Limit** functions are supported by Camera 1 only.

● Local Output

Turn on local output, you can output the video to a monitor via analog signal.

3.3.2 Configuring OSD Settings

Purpose:

OSD (On-screen Display) refers to the camera name, time/date, customized information displayed on the live view.

Note:

This function varies according to different camera models.

Steps:

1. Enter the OSD settings interface:

Configuration > Image > OSD Settings

Figure 3-15 OSD Settings

2. Check the corresponding checkbox to select the display of camera name, date or week if required.
3. Edit the camera name in the text field of **Camera Name**.
4. Select from the dropdown list to set the time format, date format and display mode.

5. You can use the mouse to drag the text frame **IPdome** in the live view window to adjust the OSD position.
6. In **Text Overlay**, you can custom 8 more text. Check the checkbox, and the corresponding text will be displayed on live image. You can click and drag the text frame to adjust position.



Figure 3-16 Adjust OSD Location

7. Click  to activate above settings.

3.3.3 Configuring Text Overlay Settings

Purpose:

You can customize the text overlay.

Steps:

1. Enter the Text Overlay settings interface:
Configuration > Image > OSD Settings
2. Check the checkbox in front of textbox to enable the on-screen display.
3. Input the characters in the textbox.
4. Use the mouse to drag the red text frame **Text** in the live view window to adjust the text overlay position.
5. Click .

Note:

There are up to 8 text overlays configurable.

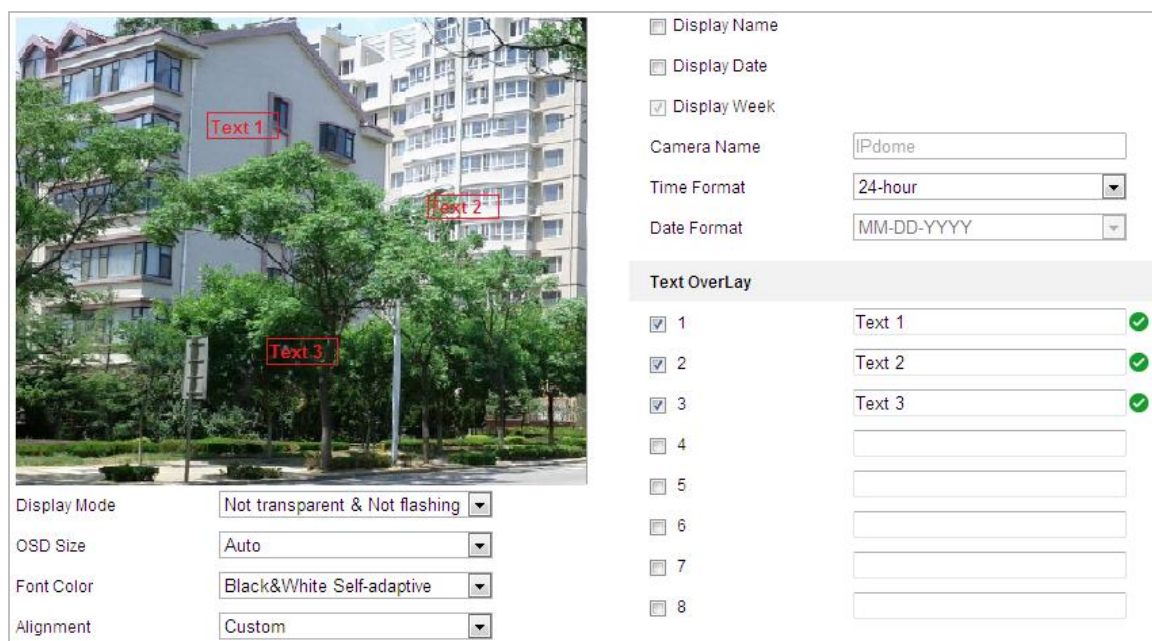


Figure 3-17 Text Overlay Settings

3.3.4 Configuring Privacy Mask for Panoramic Camera Channel

Purpose:

Privacy Mask enables you to cover certain areas on the live video to prevent certain spots in the surveillance area from being live viewed and recorded.

Note:

This function is supported by certain camera models.

Steps:

1. Enter the Privacy Mask Settings interface:
Configuration > Image > Privacy Mask
2. Check the checkbox of **Enable Privacy Mask** to enable this function.
3. Click **Draw Area**.
4. Click and drag the mouse in the live video window to draw the mask area.
5. Click **Stop Drawing** to finish drawing or click **Clear All** to clear all of the areas you set without saving them.
6. Click **Save** to save the settings.

3.4 Configuring Video and Audio Settings

Note:

Before you adjust the parameters, select the camera channel No. from the dropdown list.

3.4.1 Configuring Video Settings

Steps:

1. Enter the Video settings interface:
Configuration > Video/Audio > Video

Channel No.	Camera1	▼
Stream Type	Main Stream(Normal)	▼
Video Type	Video Stream	▼
Resolution	1920*1080P	▼
Bitrate Type	Variable	▼
Video Quality	Medium	▼
Frame Rate	25	▼ fps
Max. Bitrate	4096	Kbps
Video Encoding	H.264	▼
H.264+	OFF	▼
Profile	High Profile	▼
I Frame Interval	50	
SVC	OFF	▼
Smoothing	<input type="range"/> 50 [Clear<-->Smooth]	

Figure 3-18 Configure Video Settings

2. Select the **Stream Type** of the camera to Main Stream (Normal), Sub-Stream or Third Stream.

Note:

The main stream is usually for recording and live viewing with good bandwidth, and the sub-stream can be used for live viewing when the bandwidth is limited. Refer to the **Section 2.1 Configuring Local Parameters** for switching the stream type for live viewing.

3. You can customize the following parameters for the selected stream:

Video Type:

Select the stream type to video stream, or video & audio composite stream. The audio signal will be recorded only when the **Video Type** is **Video & Audio**.

Resolution:

Select the resolution of the video output.

Bitrate Type:

Select the bitrate type to constant or variable.

Video Quality:

When bitrate type is selected as **Variable**, 6 levels of video quality are selectable.

Frame Rate:

The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Max. Bitrate:

Set the max. bitrate. The higher value corresponds to the higher video quality, and the higher bandwidth is required as well.

Video Encoding:

Select the **Video Encoding** standard for each camera.

Profile:

You can set the profile level to **High Profile**, **Main Profile** or **Basic Profile**.

I Frame Interval:

Set the I-Frame interval from 1 to 400.

SVC:

SVC is a video encoding technology. It extracts frames from the original video and sends these frames to a video recorder which also supports SVC function when the network bandwidth is insufficient.

Smoothing:

Drag  to adjust the value of video smoothing on your demand.

Resolution Mode:

Resolution of the panoramic view channels are different in different resolution mode (including main stream, sub-stream and third stream). Select the resolution mode from the dropdown list on your demand.

Notes:

- The function is only supported by Camera 2 and Camera 3.
- Reboot the device before it takes effect when the resolution mode is switched.
- Redraw the rule area if the resolution mode is switched.

4. Click  to save the settings.

Note:

Video settings vary depending on different camera models.

3.4.2 Configuring Audio Settings

Steps:

1. Enter the Audio settings interface
Configuration > Video/Audio > Audio
2. Configure the following settings.
 - Audio Encoding:** G.722.1, G.711ulaw, G.711alaw, MP2L2, PCM and G.726 selectable.
 - Audio Stream Bitrate:** When the Audio Encoding is selected as MP2L2, you can configure the Audio Stream Bitrate in the dropdown list. The greater the value is, the better the audio quality will be.
 - Sampling Rate:** When the Audio Encoding is selected as MP2L2 or PCM, you can configure the Sampling Rate in the dropdown list. The greater the value is, the better the audio quality will be.
 - Audio Input:** When an intercom is connected to the camera, you need to set this option to **LinIn**. When a microphone is connected to the camera, you need to set this option to **MicIn**.
 - Input Volume:** Slid the bar to turn up/down the volume. The value ranges from 0 to 100.
 - Environmental Noise Filter:** When the monitoring environment is very noisy, you can enable this function to reduce part of the noise.
3. Click  to save the settings.

3.4.3 Configuring ROI Settings

Before you start:

ROI (Region of Interest) encoding is used to enhance the quality of images which are specified in advance.

Enter the ROI settings interface:

Configuration > Video/Audio > ROI

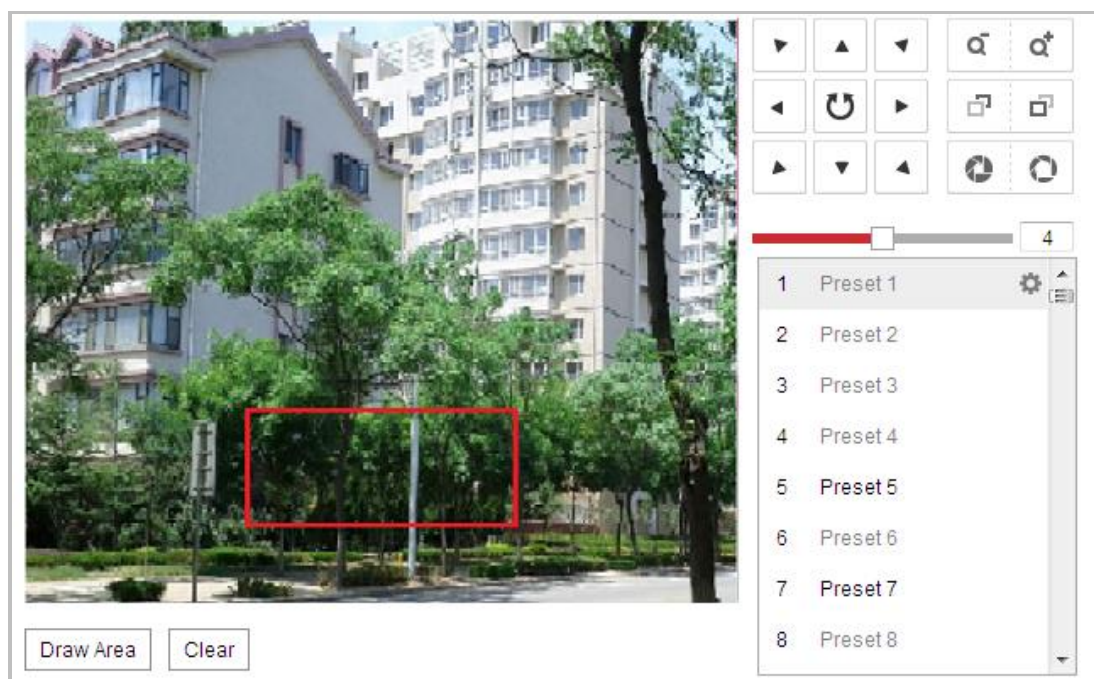


Figure 3-19 Region of Interest(1)

Stream Type	
Stream Type	Main Stream(Normal) ▼
Fixed Region	
☐ Enable	
Region No.	1 ▼
ROI Level	3 ▼
Region Name	
Dynamic Region	
☐ Enable Face Tracking	
ROI Level	3 ▼
☐ Enable Target Tracking	
ROI Level	6 ▼

Figure 3-20 Region of Interest (2)

Stream Type:

You can set the ROI function for main stream, sub-stream and third stream. Select a stream type and then configure the ROI settings.

- **Fixed Region:** The fixed region encoding is the ROI encoding for the manually configured area. And you can choose the Image Quality Enhancing level for ROI encoding, and you can also name the ROI area.

Steps:

1. Select a **Region No.**.
2. Check the **Enable** checkbox under **Fixed Region**.
3. Select the region from the dropdown list for ROI settings. There are four fixed regions selectable.

4. Click **Draw Area**, and then drag the mouse to draw the region of interest on the live video.
 5. Adjust the **ROI level** from 1 to 6. The higher the value, the better image quality in the red frame.
 6. Enter a **Region Name** and click **Save** to save the settings.
- **Dynamic Region:** The device can automatically calculate the region with motion. Set the Image Quality Enhancing level for ROI encoding.
- Steps:**
1. Check **Enable Face Tracking** and set ROI Level. Higher level means more resource is assigned to the face.
 2. Check **Enable Target Tracking** and set ROI Level. Higher level means more resource is assigned to the target.
 3. Click **Save** to save the settings.

3.4.4 Target Cropping

Purpose:

You can specify a target area on the live video, and then the specified video area can be displayed via the third stream in some certain resolution, thus to provide more details of the target area if needed.

Note:

This function varies according to different camera models.

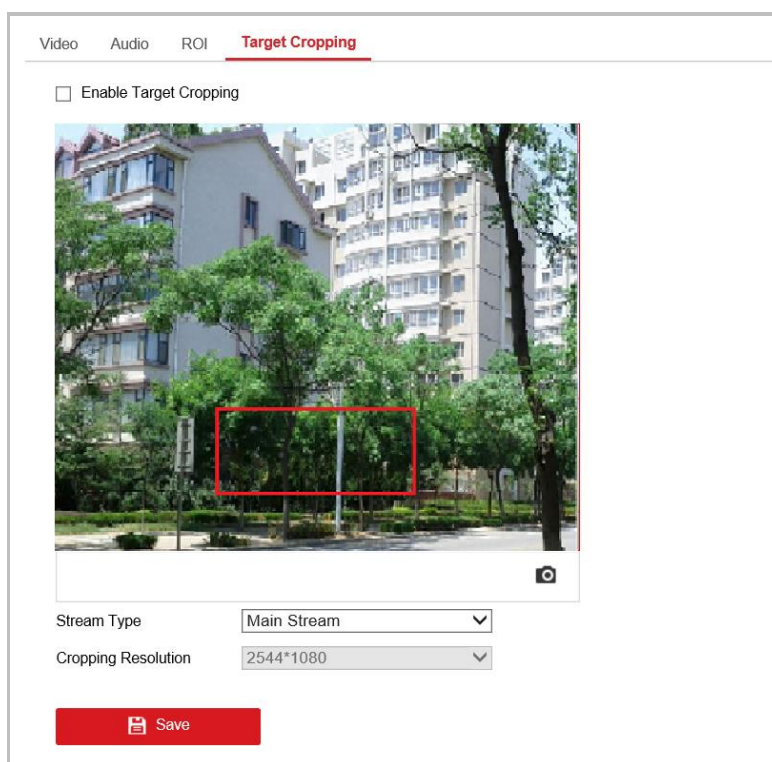


Figure 3-21 Target Cropping Configuration

Steps:

1. Enter the Target Cropping setting interface: **Configuration >Video/Audio >Target Cropping**.
2. Check **Enable Target Cropping** checkbox to enable the function.
3. Select the cropping resolution for the video display of target area. A red rectangle is displayed on the live video to mark the target area, and you can click-and-drag the rectangle to locate the target area as desired.
4. Click **Save** to save the settings.

Chapter 4 PTZ Control

4.1 Operating PTZ Control

Purpose:

In the live view interface, you can use the PTZ control buttons to control panning, tilting and zooming. Refer to **Section 3.2.2 Live View Operation** for detailed information.

4.1.1 Setting/Calling a Preset

Purpose:

A preset is a predefined image position. For the defined preset, you can click the calling button to quickly view the desired image position.

● **Setting a Preset:**

Steps:

1. In the PTZ control panel, select a preset number from the preset list.

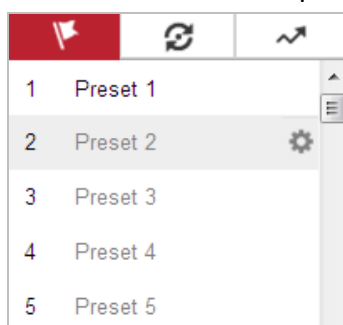


Figure 4-1 Setting a Preset

2. Use the PTZ control buttons to move the lens to the desired position.
 - Pan the camera to the right or left.
 - Tilt the camera up or down.
 - Zoom in or out.
 - Refocus the lens.
3. Click  to finish the setting of the current preset.
4. Edit a preset name by double clicking on the default name such as preset 1. (The pre-defined presets are named already and not configurable. Refer to the user manual for detailed function description.)
5. You can click  to delete the preset.

Note:

You can configure up to 300 presets.

● **Calling a Preset:**

In the PTZ control panel, select a defined preset from the list and click  to call the preset.

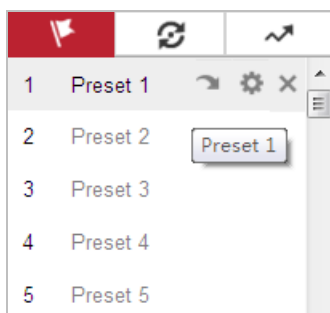


Figure 4-2 Calling a Preset

For convenient preset selection, refer to the following steps to navigate to the preset you want.

Steps:

1. Select any preset from the list.
2. Click the preset number you need on the keyboard.

Note:

The following presets are predefined with special commands. You can only call them but not configure them. For instance, preset 99 is the “Start auto scan”. If you call the preset 99, the camera starts auto scan function.

Table 4-1 Special Presets

Preset	Function	Preset	Function
33	Auto flip	93	Save manual limits
34	Back to initial position	94	Remote reboot
35	Call patrol 1	95	Call OSD menu
36	Call patrol 2	96	Stop a scan
37	Call patrol 3	97	Start random scan
38	Call patrol 4	98	Start frame scan
39	Day mode (IR cut filter in)	99	Start auto scan
40	Night mode (IR cut filter out)	100	Start tilt scan
41	Call pattern 1	101	Start panorama scan
42	Call pattern 2	102	Call patrol 5
43	Call pattern 3	103	Call patrol 6
44	Call pattern 4	104	Call patrol 7
45	One-touch patrol	105	Call patrol 8
92	Set manual limits		

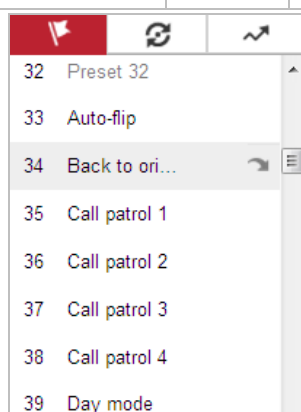


Figure 4-3 Special Preset

Note:

You may need to use the OSD (On Screen Display) menu when controlling the camera remotely. To display the OSD menu on the live view screen, you can call the preset number 95.

4.1.2 Setting/Calling a Patrol

Purpose:

A patrol is a memorized series of preset function. It can be configured and called on the patrol settings interface. There are up to 8 patrols for customizing. A patrol can be configured with 32 presets.

Before you start:

Make sure that the presets you want to add into a patrol have been defined.

- **Setting a Patrol:**

Steps:

1. In the PTZ control panel, click  to enter the patrol settings interface.
2. Select a patrol number from the list and click .
3. Click  to enter the adding interface of preset, as shown in Figure 4-4.



Figure 4-4 Adding Presets

4. Configure the preset number, patrol time and patrol speed.

Table 4-2 Patrol Time and Patrol Speed

Name	Description
Patrol Time	It is the duration staying on one patrol point. The camera moves to another patrol point after the patrol time.
Patrol Speed	It is the speed of moving from one preset to another.

5. Click **OK** to save a preset into the patrol.
6. Repeat the steps from 3 to 5 to add more presets.
7. Click **OK** to save all the patrol settings.

- **Calling a Patrol:**

In the PTZ control panel, select a defined patrol from the list and click  to call the patrol, as shown in Figure 4-5.

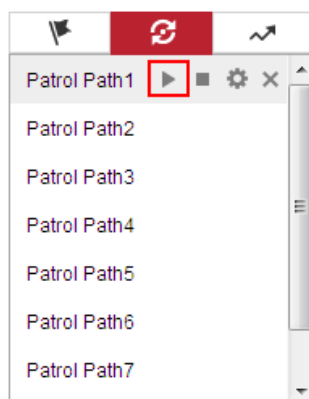


Figure 4-5 Calling a Patrol

4.1.3 Setting/Calling a Pattern

Purpose:

A pattern is a memorized series of pan, tilt, zoom, and preset functions. It can be called on the pattern settings interface. There are up to 4 patterns for customizing.

● **Setting a Pattern:**

Steps:

1. In the PTZ control panel, click  to enter the pattern settings interface.
2. Select a pattern number from the list as shown in Figure 4-6.

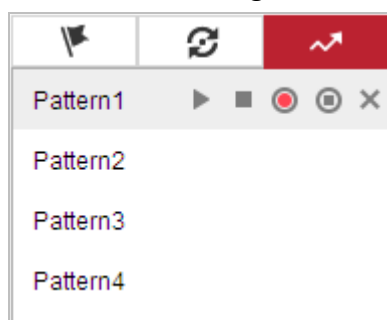


Figure 4-6 Patterns Settings Interface

3. Click  to enable recording the panning, tilting and zooming actions.
4. Use the PTZ control buttons to move the lens to the desired position after the information of **Program Pattern Remaining Memory (%)** is displayed on the screen.
 - Pan the camera to the right or left.
 - Tilt the camera up or down.
 - Zoom in or out.
 - Refocus the lens.
5. Click  to save all the pattern settings.

Notes:

- These 4 patterns can be operated separately and with no priority level.
- When configuring and calling the pattern, proportional pan is valid; the limit stops and auto flip will be invalid; and the 3D positioning operation is not supported.

4.2 PTZ Configuration

4.2.1 Configuring Basic PTZ Parameters

Purpose:

You can configure the basic PTZ parameters, including proportional pan, preset freezing, preset speed, etc.

1. Enter the Basic PTZ parameter configuration interface:

Configuration > PTZ > Basic Settings

Basic Parameter	
☒	Enable Proportional Pan
☐	Enable Preset Freezing
Preset Speed	4
Manual Control Speed	Auto
Keyboard Control Speed	Medium
Auto Scan Speed	28
Max. Tilt-angle	(0 - 90)Degree
Zooming Speed	3
PTZ OSD	
Zoom Status	2s
PT Status	2s
Preset Status	2s
Power Off Memory	
Set Resume Time Point	30s

Figure 4-7 Basic PTZ Configuration Interface

2. Configure the following settings:

- ◆ **Basic Parameters:** Enable/disable proportional pan and preset freezing, set the preset speed, manual control speed, keyboard control speed, auto scan speed, and zooming speed.
 - **Proportional Pan:** If you enable this function, the pan/tilt speeds change according to the amount of zoom. When there is a large amount of zoom, the pan/tilt speed will be slower for keeping the image from moving too fast on the live view image.
 - **Preset Freezing:** This function enables the live view to switch directly from one scene defined by a preset to another, without showing the middle areas between these two, to ensure the surveillance efficiency. It can also reduce the use of bandwidth in a digital network system.
- Note:**
Preset freezing function is invalid when you calling a pattern.
- **Preset Speed:** You can set the speed of a defined preset from 1 to 8.
- **Manual Control Speed:** The manual control speed can be set as Compatible, Pedestrian, Non-motor Vehicle, Motor Vehicle or Auto.
 - Compatible: The control speed is same as the Keyboard Control Speed.
 - Pedestrian: Choose the **Pedestrian** when you monitor the pedestrians.

- **Non-motor Vehicle:** Choose the **Non-motor Vehicle** when you monitor the non-motor vehicles.
 - **Motor Vehicle:** Choose the **Motor Vehicle** when you monitor the motor vehicles.
 - **Auto:** You are recommended to set it to be auto when the application scene of the camera is complicated.
 - **Keyboard Control Speed:** Define the speed of PTZ control by a keyboard as Low, Medium or High.
 - **Auto Scan Speed:** The scan speed can be set from level 1 to 40.
 - **Max. Tilt-angle:** Set the tilt-angle of the speed dome from the drop-down list.
 - **Zooming Speed:** The zoom speed is adjustable from level 1 to 3.
 - ◆ **PTZ OSD:** Set the on-screen display duration of the PTZ status.
 - **Zoom Status:** Set the OSD duration of zooming status as 2 seconds, 5 seconds, 10 seconds, Always Close or Always Open.
 - **PT Status:** Set the azimuth angle display duration while panning and tilting as 2 seconds, 5 seconds, 10 seconds, Always Close or Always Open.
 - **Preset Status:** Set the preset name display duration while calling the preset as 2 seconds, 5 seconds, 10 seconds, Always Close or Always Open.
 - ◆ **Power-off Memory:** The camera can resume its previous PTZ status or actions after it restarted from a power-off. You can set the time point of which the camera resumes its PTZ status. You can set it to resume the status of 30 seconds, 60 seconds, 300 seconds or 600 seconds before power-off.
3. Click  to save the settings.

4.2.2 Configuring PTZ Limits

Purpose:

The camera can be programmed to move within the configurable PTZ limits (left/right, up/down).

Steps:

1. Enter the Limit configuration interface:
Configuration > PTZ > Limit

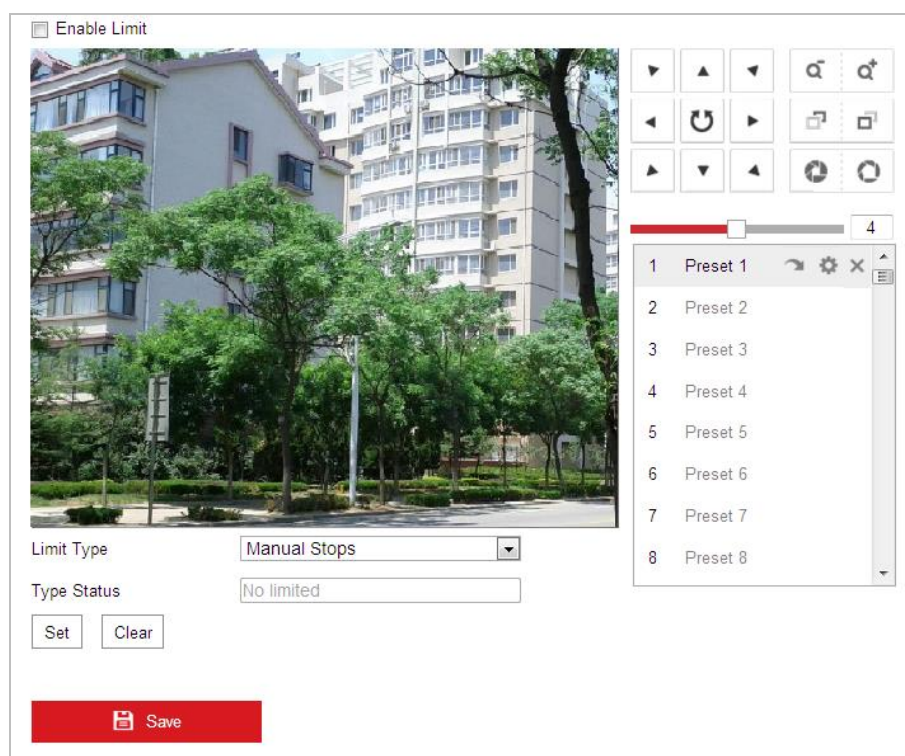


Figure 4-8 Configure the PTZ Limit

2. Click the **Enable Limit** checkbox and choose the limit type as manual stops or scan stops.
 - **Manual Stops:**
When manual limit stops are set, you can operate the PTZ control panel manually only in the limited surveillance area.
 - **Scan Stops:**
When scan limit stops are set, the random scan, frame scan, auto scan, tilt scan, panorama scan is performed only in the limited surveillance area.
- Note:**
Manual Stops of **Limit Type** is prior to **Scan Stops**. When you set these two limit types at the same time, **Manual Stops** is valid and **Scan Stops** is invalid.
3. Click the PTZ control buttons to find the left/right/up/down limit stops; you can also call the defined presets and set them as the limits of the camera.
4. Click **Set** to save the limits or click **Clear** to clear the limits.

4.2.3 Configuring Initial Position

Purpose:

The initial position is the origin of PTZ coordinates. It can be the factory default initial position. You can also customize the initial position according to your own demand.

◆ **Customize an Initial Position:**

Steps:

1. Enter the Initial Position configuration interface:
Configuration > PTZ > Initial Position

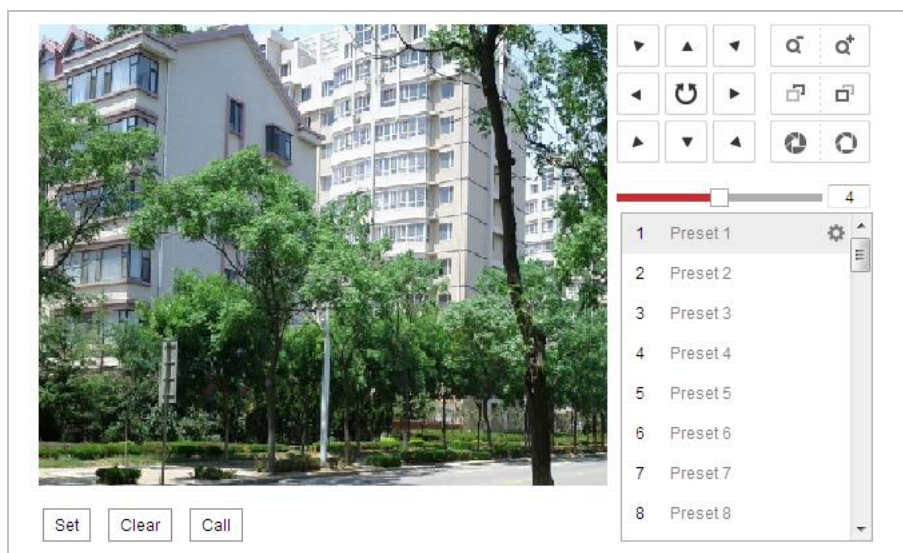


Figure 4-9 PTZ Configuration

2. Click the PTZ control buttons to find a position as the initial position of the camera; you can also call a defined preset and set it as the initial position of the camera.
3. Click **Set** to save the position.

◆ **Call/delete an Initial Position:**

You can click  to call the initial position. You can click  to delete the initial position and restore the factory default initial position.

4.2.4 Configuring Park Action

Purpose:

This feature allows the camera to start a predefined park action (scan, preset, pattern and etc.) automatically after a period of inactivity (park time). The park action function only takes effect in Camera 1.

Note:

Scheduled Tasks function is prior to **Park Action** function. When these two functions are set at the same time, only the **Scheduled Tasks** function takes effect.

Steps:

1. Enter the Park Action settings interface:

Configuration > PTZ > Park Action

Figure 4-10 Set the Park Action

2. Check the **Enable Park Action** checkbox.
3. Set the **Park Time** as the inactivity time of the camera before it starts the park actions.
4. Choose **Action Type** from the dropdown list.

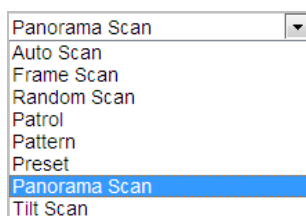


Figure 4-11 Action Types

5. Click  to save the settings.

4.2.5 Configuring Privacy Mask for PTZ Camera Channel

Purpose:

Privacy mask enables you to cover certain areas on the live video to prevent certain spots in the surveillance area from being live viewed and recorded. The privacy mask function only takes effect in Camera 1.

Steps:

1. Enter the Privacy Mask settings interface:

Configuration > PTZ > Privacy Mask

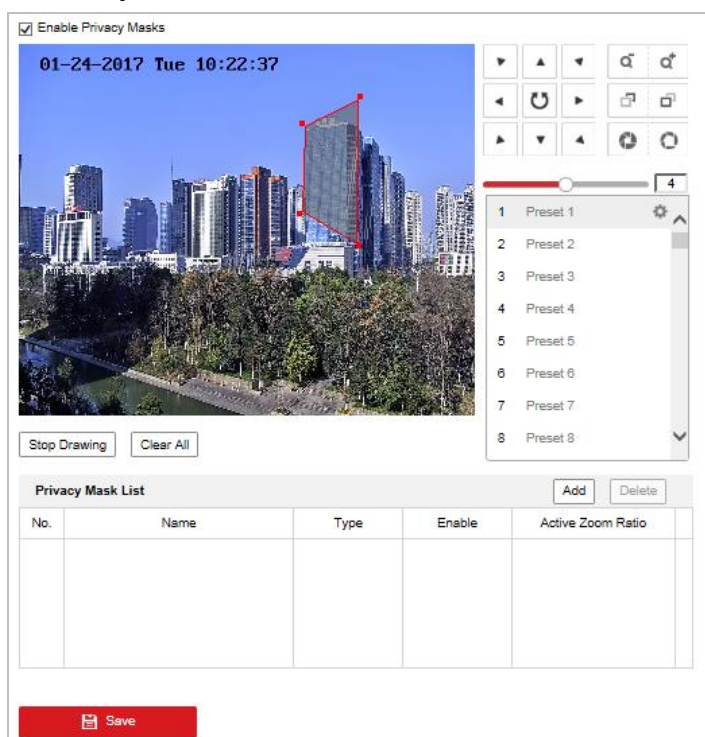
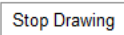


Figure 4-12 Draw the Privacy Mask

2. Click the PTZ control buttons to find the area you want to set the privacy mask.
3. Click ; drag the mouse in the live video window to draw the area.
You can drag the corners of the red rectangle area to draw a polygon mask.
4. Click  to finish drawing or click  to clear all of the areas you set without saving them.

5. Click **Add** to save the privacy mask, and it will be listed in the **Privacy Mask List** area; set the value of **Active Zoom Ratio** on your demand, and then the mask will only appear when the zoom ratio is greater than the predefined value.

Privacy Mask List					Add	Delete
No.	Name	Type	Enable	Active Zoom Ratio		
1	Privacy Mask 1	gray	Yes	1		

Figure 4-13 Privacy Mask List

6. you can also define the color of the masks.



Figure 4-14 Define Mask Color

7. You can select a mask and click **Delete** to delete it from the list.
8. Check the **Enable Privacy Mask** checkbox to enable this function.

Note:

You are allowed to draw up to 24 areas on the same image.

4.2.6 Configuring Scheduled Tasks

Purpose:

You can configure the network camera to perform a certain action automatically in a user-defined time period.

Steps:

- Enter the Scheduled Task settings interface:
Configuration > PTZ > Scheduled Tasks

Enable Scheduled Task

OFF ✕ Delete 🗑 Delete All

Mon 0 2 4 6 8 10 12 14 16 18 20 22 24

Tue 0 2 4 6 8 10 12 14 16 18 20 22 24

Wed 0 2 4 6 8 10 12 14 16 18 20 22 24

Thu 0 2 4 6 8 10 12 14 16 18 20 22 24

Fri 0 2 4 6 8 10 12 14 16 18 20 22 24

Sat 0 2 4 6 8 10 12 14 16 18 20 22 24

Sun 0 2 4 6 8 10 12 14 16 18 20 22 24

Park Time s

💾 Save

- OFF
- Auto Scan
- Frame Scan
- Random Scan
- Patrol
- Pattern
- Preset
- Panorama Scan
- Tilt Scan
- Dome Reboot
- Dome Adjust
- Aux Output

Figure 4-15 Configure Scheduled Tasks

2. Check the **Enable Scheduled Task** checkbox.
3. Set the **Park Time**. You can set the park time (a period of inactivity) before the camera starts the scheduled tasks.
4. Select the task type from the dropdown list. You can choose scan, preset, pattern and etc.

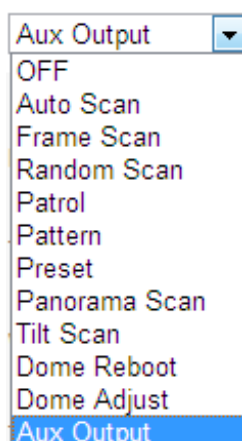


Figure 4-16 Task Types

5. Select the timeline of a certain day, and drag the left button of the mouse to set the recording schedule (the start time and end time of the recording task).
6. (Optional) After you set the scheduled task, you can click  and copy the task to other days.



Figure 4-17 Edit the Schedule and Task Type

- After setting the record schedule, you can click a record segment to display the segment record settings interface to edit the segment record parameters. (Optional)

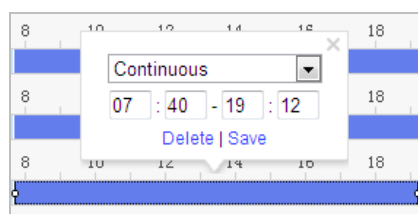


Figure 4-18 Segment Record Settings

Note:

The time of each task cannot be overlapped. Up to 10 tasks can be configured for each day.

- Click  to save the settings.

4.2.7 Clearing PTZ Configurations

Purpose:

You can clear PTZ configurations in this interface, including all presets, patrols, patterns, privacy masks, PTZ limits, scheduled tasks and park actions.

Steps:

- Enter the Clearing Configuration interface:
Configuration > PTZ > Clear Config
- Check the checkbox of the items you want to clear.
- Click  to clear the settings.

4.2.8 Configuring PTZ Control Priority

Steps:

- Get to the configuration interface:
Configuration > PTZ > Prioritize PTZ.

- The camera can be controlled by network and RS-485 signals. You can set the control priority of these two signals.
- The operation of **Operator** is prior to that of **User**. When the **Operator** is controlling the camera, the **User** cannot control it. When the **Operator** finishes, the **User** can control the camera after the **Delay** time. The **Delay** time can be set in Priority PTZ interface as shown follows.

Figure 4-19 PTZ Priority

2. Click  to activate the settings.

4.2.9 Configuring Panorama Tracking

Purpose:

After you enable this function, when the camera detects the moving object in the panoramic view, the PTZ camera channel will track the detected target. PTZ camera channel automatically adjusts its PTZ position to ensure that the target is in the center of PTZ view with certain detailed information. When you need to perform the manual tracking, click the icon of live view interface and click the target to start tracking.

Steps:

1. Enter the Panorama Tracking settings interface:

Configuration > PTZ > Panorama Tracking

No.	Coordinate(x, y)	PTZ Position(p, t, z)
1	(254, 623)	(276, 17, 1)
2	(89, 666)	(267, 13, 1)
3	(576, 339)	(293, 40, 1)
4	(239, 196)	(268, 50, 1)
5	(458, 800)	(267, 4, 1)
6	(760, 226)	(307, 48, 1)

Note: Auto calibrating can be performed independently for every scene. After auto calibrating done for all scenes, reboot the device to activate the new settings.

Figure 4-20 Configure Panorama Tracking

2. Check the **Enable Tracking** checkbox to enable panorama tracking function.
3. Select the calibration mode and perform the calibration.

Auto Calibration:

- (1) Select the calibration mode as **Auto**.
- (2) Select mode for auto calibration: One-Touch Calibration and Single Scene Calibration.
 - For one-touch calibration, camera performs automatically after clicking the button.
 - For single-scene calibration, camera performs calibration scene by scene with a bit human help.
 - i. Move and zoom in/out the PTZ camera channel to make sure the PTZ view and panoramic view is mostly the same.
 - ii. Click **Start Calibration** to start the calibration. After calibration for one scene is done, manually change to another scene to perform further calibration.
- (3) Set the tracking duration: the PTZ camera channel stops tracking after the set duration.
- (4) Set the zoom ratio: Set the zoom ratio of PTZ camera channel manually to ensure the certain scale of target in the PTZ view. The PTZ camera channel tracks the target by the scale once the tracking is triggered.
- (5) Click Set Zoom Ratio to set the current zoom ratio as the tracking zoom ratio.
- (6) After calibration for all scenes are done, click Auto Calibration Succeeded. The device reboots automatically to take effect.

Manual Calibration:

- (1) Select the calibration mode as **Manual**.
- (2) Move the No.1 site of panoramic view to certain site “” and set the calibration site.
- (3) Move and zoom in/out the Camera 02 to make sure the  of PTZ view and the  of panoramic view are at the same position. You can use  to quickly locate the desired point.
 - i. Click  to enable the function.
 - ii. Click the same point as the numbered cross marked on panoramic camera channel.
The PTZ camera place the clicked point in the middle of the image automatically.
 - iii. Click the button again to turn it off.
- (4) Click  to save current ptz position and show in the calibration parameter list.
- (5) Repeat the steps above to add more calibration points for the Panorama View (Scene#).
- (6) Set Tracking Initial: When the camera finish calibrating or has a calibration timeout, close-up view shall turn to a fixed position. Click the PTZ button to set a certain position, then click **Set Tracking Initial** to finish setting.
- (7) Set the tracking duration: the PTZ camera channel stops tracking after the set duration.
- (8) Set the zoom ratio: Set the zoom ratio of PTZ camera channel manually to ensure the certain scale of target in the PTZ view. The PTZ camera channel tracks the target by the scale once the tracking is triggered.
- (9) Click **Set Zoom Ratio** to set the current zoom ratio as the tracking zoom ratio.
- (10) Click  and repeat above steps to move on to set calibration points for the next scene.
- (11) Click **Start Calibration**.

Notes:

- Up to 12 calibration points are supported for each scene. At least 4 points should be configured. More calibration points can increase the rate for successful calibration.
- Scatter the calibration points evenly in live view image for better calibration effect.

4. Save the settings.

Calibration Parameter			Add	Delete	Clear Coordin...
No.	Coordinate(x, y)	PTZ Position(p, t, z)			
1	(254, 623)	(276, 17, 1)			
2	(89, 666)	(267, 13, 1)			
3	(576, 339)	(293, 40, 1)			
4	(239, 196)	(268, 50, 1)			
5	(458, 800)	(287, 4, 1)			
6	(760, 226)	(307, 48, 1)			

Figure 4-21 Calibration Parameters

Notes:

- In auto calibration mode, the more similar is the PTZ view and the panoramic view, the panorama tracking gets more accurate.
- The more distant manual calibration sites are to each other, the panorama tracking gets more accurate.

4.2.10 Rapid Focus

Purpose:

After this function is enabled, perform calibration and the focus can be quicker than quick focus.

Steps:

1. Enter the Position Settings interface:
Configuration > PTZ > Position Settings.
2. Check the Enable checkbox to enable the Rapid Focus.
3. Drag the red line on the live view image to the calibration position according to the user. You can drag the ends of the red line to adjust the length of the line.
4. Click Start Calibration. There is the notice Calibrating on the live view image and the camera lens performs auto focus.
5. After calibration, there is the notice Calibration succeeded on the live view image.
6. Click Save to save the settings.
7. You can repeat step 3 to step 6 to configure rapid focus for multiple scenes. Up to four scenes are supported.

Chapter 5 Storage and Playback

Notes:

- In this and the following chapters, operation of the camera by the web browser will be taken as an example.
- You can set recording and capture schedule for different channels of the camera. Refer to the actual configuration interface.

5.1 Storage Settings

Before you start:

To configure record settings, make sure that you have the network storage device within the network or the memory card has been inserted in the corresponding card slot. Refer to the quick start guide for the location of the memory card slot.

5.1.1 Configuring Net HDD

Before you start:

The network disk should be available within the network and properly configured to store the recorded files, log files, etc.

Steps:

Add Net HDD

1. Enter the NAS (Network-Attached Storage) settings interface:

Configuration > Storage > Storage Management > Net HDD

HDD No.	Server Address	File Path	Type	Delete
1	10.10.36.61	/cxy_1	NAS	✗
2	10.10.36.252	/dvr/yangjian_1	NAS	✗
3			NAS	✗

Mounting Type: User Name: Password:

Figure 5-1 Select Net HDD Type

2. Input the IP address of the network disk, and input the file path.
3. Select the mounting type. NFS and SMB/CIFS are selectable. You can set the user name and password to guarantee the security if SMB/CIFS is selected.

Note:

Refer to the *NAS User Manual* for creating the file path.



- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (Using a minimum of 8 characters, including at least three of

the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product.

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- If the status of the disk is *Uninitialized*, check the corresponding checkbox to select the disk and click **Format** to start initializing the disk.
 - Click  to save the settings.

5.1.2 HDD Management

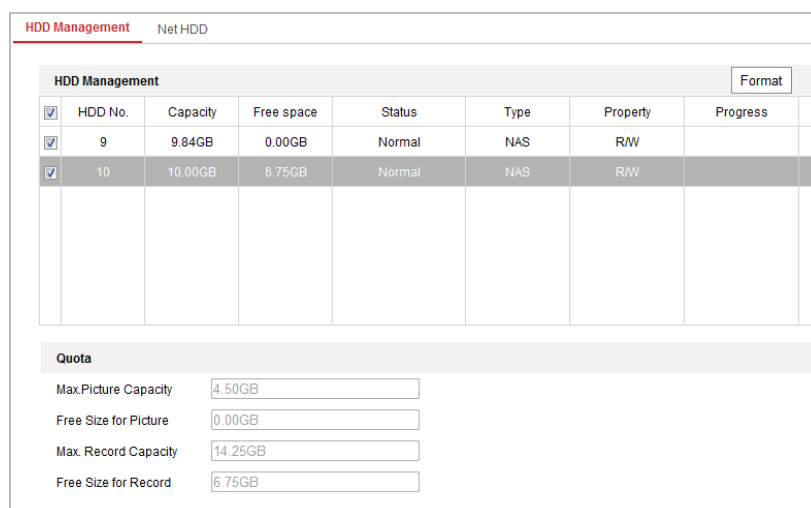
If the memory card is inserted in the device or NAS (Network-Attached Storage) is added, enter HDD Management interface to configure the storage status.

Steps:

- Enter the HDD settings interface

Configuration > Storage > Storage Management > HDD Management,

You can view the capacity, free space, status, type and property of the disk.



The screenshot shows the 'HDD Management' interface. At the top, there's a 'Format' button. Below it is a table with columns: HDD No., Capacity, Free space, Status, Type, Property, and Progress. Two disks are listed: HDD No. 9 (9.84GB, 0.00GB, Normal, NAS, R/W) and HDD No. 10 (10.00GB, 6.75GB, Normal, NAS, R/W). Below the table is a 'Quota' section with four input fields: Max. Picture Capacity (4.50GB), Free Size for Picture (0.00GB), Max. Record Capacity (14.25GB), and Free Size for Record (6.75GB).

Figure 5-2 Storage Management Interface

- If the status of the disk is **Uninitialized**, check the corresponding checkbox to select the disk and click **Format** to start initializing the disk.
- When the initialization completed, the status of disk will become **Normal**.

HDD Management							Set	Format
☒	HDD No.	Capacity	Free space	Status	Type	Property	Progress	
☒	9	20.00GB	0.00GB	Formatting	NAS	R/W		

Figure 5-3 View Disk Status

Define the Quota for Record and Pictures

Steps:

- Input the quota percentage for picture and for record.
- Click **Save** and refresh the browser page to activate the settings.

Quota

Max. Picture Capacity: 4.75GB

Free Size for Picture: 4.75GB

Max. Record Capacity: 14.50GB

Free Size for Record: 14.50GB

Percentage of Picture: 25%

Percentage of Record: 75%

Save

Figure 5-4 Quota Settings

Note:

Up to 8 NAS disks can be connected to the camera.

5.1.3 Configuring Record Schedule

Before you start:

Make sure a local memory card is inserted in the camera or the network storage is added to the camera.

Purpose:

There are two kinds of recording for the cameras: manual recording and scheduled recording. In this section, you can follow the instructions to configure the scheduled recording. By default, the record files of scheduled recording are stored in the memory card (if supported) or in the network disk.

Steps:

1. Enter the Record Schedule settings interface:

Configuration > Storage > Schedule Settings > Record Schedule

Record Schedule Capture

Channel No. Camera 1

☐ **Enable**

Continuous ✕ Delete 🗑️ Delete All Advanced

Mon 0 2 4 6 8 10 12 14 16 18 20 22 24

Tue 0 2 4 6 8 10 12 14 16 18 20 22 24

Wed 0 2 4 6 8 10 12 14 16 18 20 22 24

Thu 0 2 4 6 8 10 12 14 16 18 20 22 24

Fri 0 2 4 6 8 10 12 14 16 18 20 22 24

Sat 0 2 4 6 8 10 12 14 16 18 20 22 24

Sun 0 2 4 6 8 10 12 14 16 18 20 22 24

Continuous Motion Event

Copy to... Save

Figure 5-5 Record Schedule Interface

2. Check the **Enable** checkbox to enable scheduled recording.
3. To set the advanced settings of the camera, click Advanced to enter the advanced settings interface.

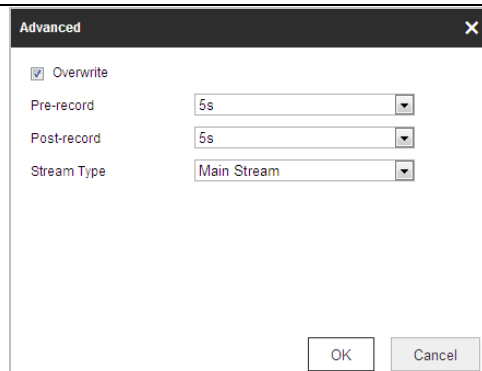


Figure 5-6 Record Parameters

- **Pre-record:** The time you set to start recording before the scheduled time or the event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts to record at 9:59:55.

The Pre-record time can be configured as No Pre-record, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s or not limited.

Note:

The pre-record time changes according to the video bitrate.

- **Post-record:** The time you set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.

The Post-record time can be configured as 5 s, 10 s, 30 s, 1 min, 2 min, 5 min or 10 min.

Note:

The Pre-record and Post-record parameters vary depending on different camera models.

- **Stream Type:** You can select the stream type for recording; Main stream, sub stream and third stream are selectable. If you select the sub stream, you can record for a longer time with the same storage capacity.
 - **Overwrite:** If you enable this function and the HDD is full, the new record files overwrite the oldest record files automatically.
4. Click **OK** to save the advanced setting.



Figure 5-7 Record Schedule

5. Set the record schedule:
- (1) Select a **Record Type**. The record type can be Continuous, Motion, Alarm, Motion | Alarm, Motion & Alarm, and Event.
- **Continuous**

If you select **Continuous**, the video will be recorded automatically according to the time of the schedule.

- **Record Triggered by Motion Detection**

If you select **Motion**, the video will be recorded when the motion is detected.

Besides configuring the recording schedule, you have to set the motion detection area and check the **Trigger Channel** checkbox in the **Linkage Method** of Motion Detection settings interface. For detailed information, refer to the *Step 1 in the Section 6.1.1 Configuring Motion Detection*.

- **Record Triggered by Alarm**

If you select **Alarm**, the video will be recorded when the alarm is triggered via the external alarm input channels.

Besides configuring the recording schedule, you have to set the **Alarm Type** and check the **Trigger Channel** checkbox in the **Linkage Method** of **Alarm Input Settings** interface. For detailed information, refer to *Section 6.1.3 Configuring Alarm Input*.

- **Record Triggered by Motion | Alarm**

If you select **Motion | Alarm**, the video will be recorded when the external alarm is triggered or the motion is detected.

Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input** settings interfaces. Refer to *Section 6.1.1* and *Section 6.1.3* for detailed information.

- **Record Triggered by Motion & Alarm**

If you select **Motion & Alarm**, the video will be recorded when the motion and alarm are triggered at the same time.

Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input** settings interfaces. Refer to *Section 6.1.1* and *Section 6.1.3* for detailed information.

- **Record Triggered by Audio Exception Detection:** If you select **Audio Exception Detection**, the video will be recorded when the audio exception detection is triggered. Besides configuring the recording schedule, you have to configure the *Audio Exception Detection*.
- **Record Triggered by VCA events:** If you select **VCA**, the video will be recorded when the either of the VCA events is triggered. Besides configuring the recording schedule, you have to configure the VCA.
- **Record Triggered by smart events:** The smart events include Line Crossing Detection, Intrusion Detection, Region Entrance Detection and Region Exiting Detection. If you select to record by one type of the smart events, the video will be recorded when the selected smart event is triggered. Besides configuring the recording schedule, you have to configure the specific event settings.
- **Record Triggered by All Events:** If you select **Event**, the video will be recorded when any event is detected.

Note:

Either the smart events or the VCA events are supported, which varies depending on the camera models.

6. Select the record type, and drag the mouse on the time bar to set the record schedule.

7. Click  to save the settings.

5.1.4 Configuring Capture Schedule

Purpose:

You can configure the scheduled snapshot and event-triggered snapshot. The captured picture can be stored in the local storage or network storage.

Steps:

1. Enter the Capture settings interface:

Configuration > Storage > Storage Settings > Capture

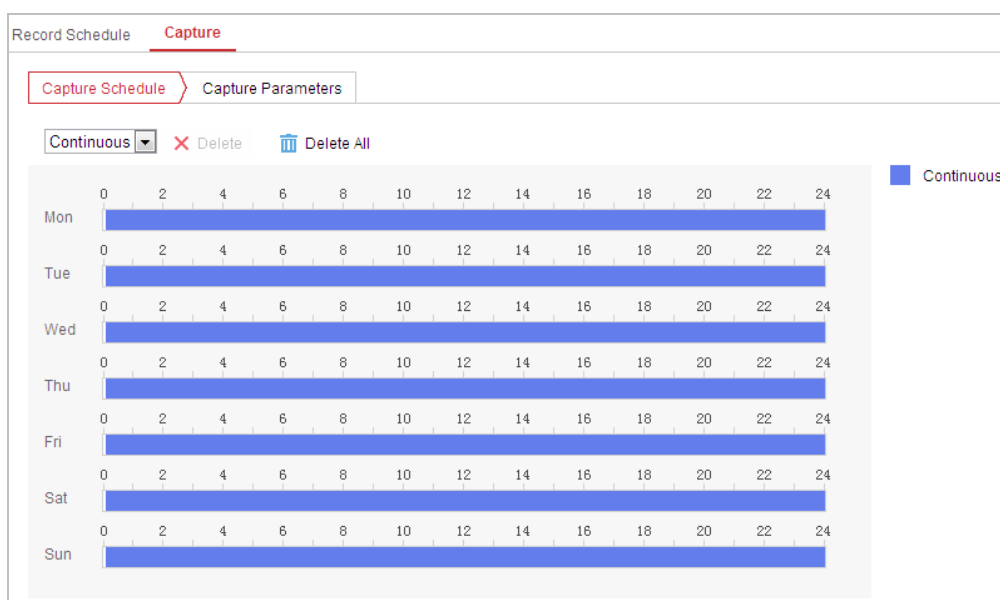


Figure 5-8 Snapshot Settings

2. Click **Capture Schedule** to enter the Capture interface.
3. Select the timeline of a certain day, and drag the left button of the mouse to set the capture schedule (the start time and end time of the recording task).
4. After you set the scheduled task, you can click  and copy the task to other days (optional).
5. After setting the capture schedule, you can click a capture segment to display the segment capture settings interface to edit the segment capture parameters. (optional)

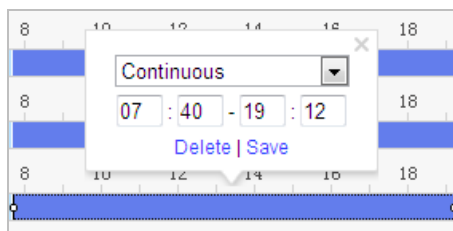


Figure 5-9 Segment Snapshot Settings

6. Click **Capture Parameters** to enter the Capture Parameters interface.
7. Check the **Enable Timing Snapshot** checkbox to enable continuous snapshot, and configure the schedule of timing snapshot. Check the **Enable Event-triggered Snapshot** checkbox to enable event-triggered snapshot.
8. Select the format, resolution, quality of the snapshot.
9. Set the time interval between two snapshots.

10. Click  to save the settings.

5.1.5 Cloud Storage

Purpose:

The captured pictures can be saved on Cloud Storage when the function is configured.

Note:

Cloud storage function varies according to different camera models.

Steps:

1. Check the checkbox of Enable Cloud Storage.
2. Select a protocol version.
3. Input the IP address and port of the storage server.
4. Input the user name, password and confirm password for the authentication of the storage server if you select the protocol version as Cloud1.0. Input AccessKey and SecretKey if you select the protocol version as Cloud2.0.
5. Input picture storage pool ID on the server.
6. (Optional) You can click Test to test the cloud storage settings.
7. Click Save to save the settings.

Note:

The storage server port ranges from 2000 to 65535 and the picture storage pool ID ranges from 1 to 255.

5.2 Picture

Purpose:

This section explains how to view the captured picture files stored in the network disks and download the captured pictures.

Steps:

1. Click  on the menu bar to enter picture interface.

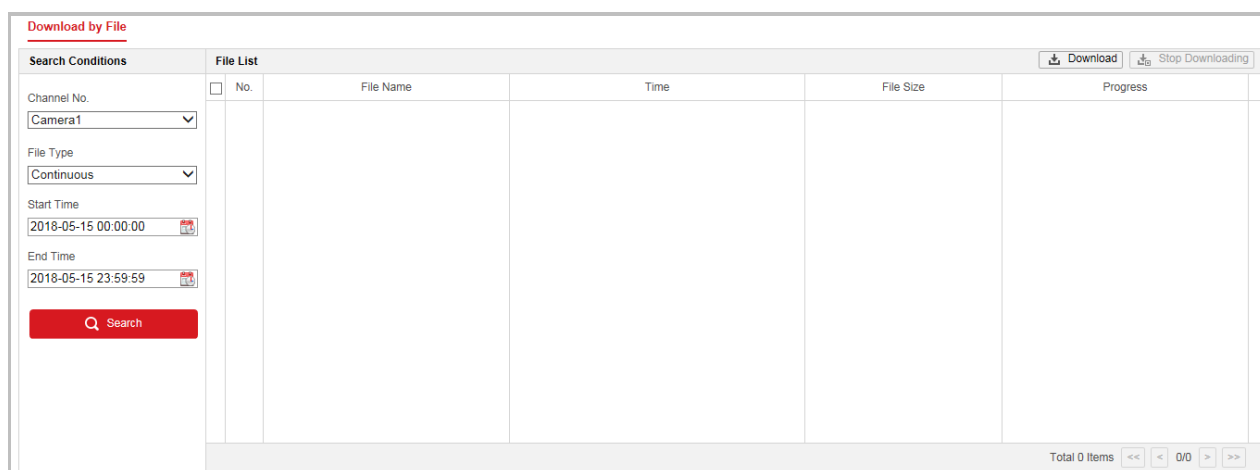


Figure 5-10 Picture Interface

2. Select the search conditions, including the picture type, start time, and end time, then click **Search**. The results will be listed on the picture list area.

3. Select one picture and click **Preview** to preview the picture.
4. Check the checkbox in front of the files that you need to download.
5. Click  **Download** to download the files.

Note:

Configure the saving path from **Configuration > Local Configuration > Save** snapshots in live view.

5.3 Playback

Purpose:

This section explains how to view the remotely recorded video files stored in the memory card or network disks.

5.3.1 Play Back Video Files

Steps:

1. Click  on the menu bar to enter playback interface.

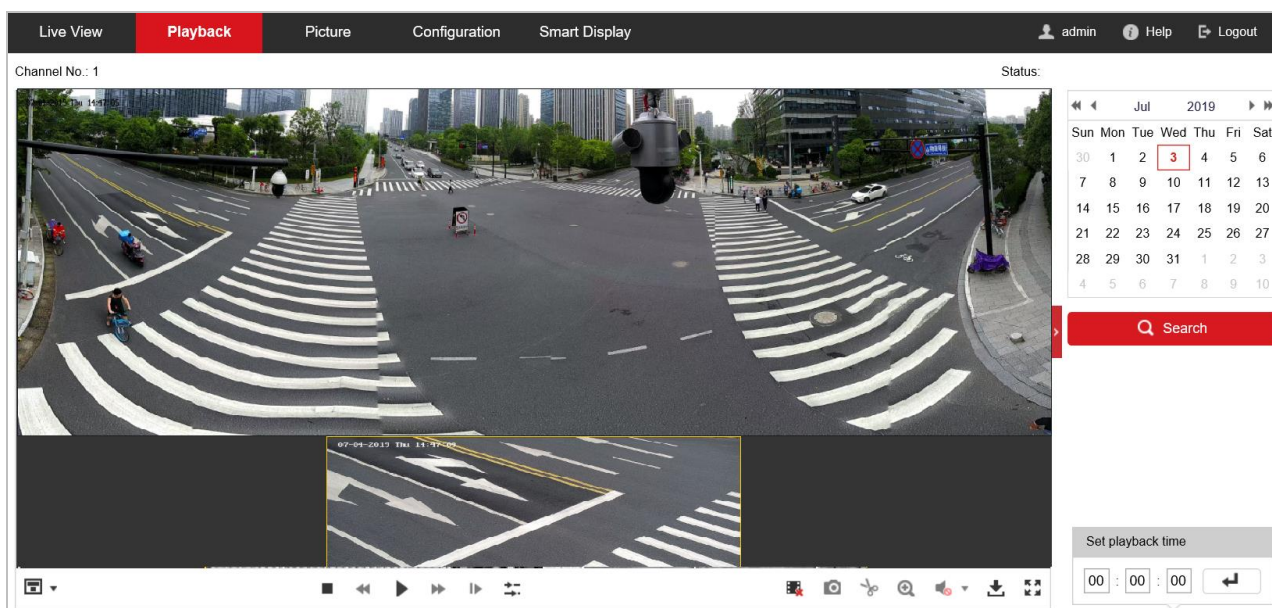
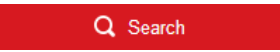


Figure 5-11 Playback Interface

2. Select the date and click .

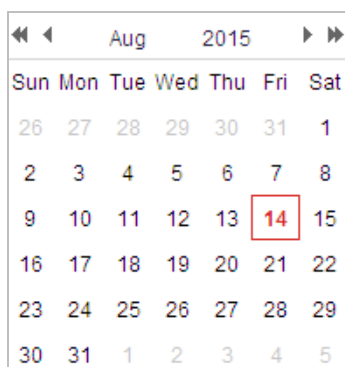


Figure 5-12 Search Video

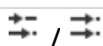
3. Click  to play the video files found on this date.

The toolbar on the bottom of Playback interface can be used to control playing process.



Figure 5-13 Playback Toolbar

Descriptions of Icons on PTZ Control Panel are listed below:

Playback		Click  to start playback and the icon turns into  . Click the icon again to stop playback.
		Stop All Playback Click  to stop all channels's playback at once.
		Single Frame Click  to start playback by frame.
Playing Speed		Click  to slow forward and click  to fast forward.
Synchronous Playback		Click  to playback videos synchronously, and click  to stop synchronous playback.
Capture a picture		Click  to manually capture the picture.
Clip		Click  to start clipping video file and the icon turns into  . Click the icon again to stop clipping.
Digital Zoom		Click  to enable digital zoom function and the icon turns into  . Then scroll the mouse wheel up/down to zoom in/out the live view image.
Download		Click  to download the video file.

Note:

You can choose the file paths locally for downloaded playback video files and pictures in Local Configuration interface. Refer to **Section 2.1** for details.

Drag the progress bar with the mouse to locate the exact playback point. You can also input the time and click  to locate the playback point in the **Set playback time** field. You can also click   to zoom out/in the progress bar.

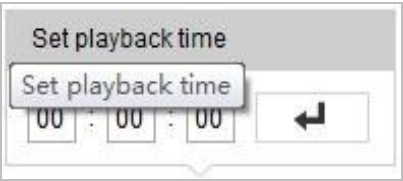


Figure 5-14 Set Playback Time



Figure 5-15 Progress Bar

The different colors of the video on the progress bar stand for the different video types as shown in Figure 5-16.

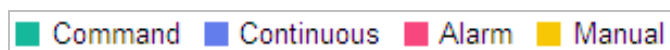


Figure 5-16 Video Types

5.3.2 Downloading Video Files

Steps:

1. Click  on the playback interface. The pop-up menu is shown in Figure 5-17.
2. Set the start time and end time. Click **Search**. The corresponding video files will be listed.

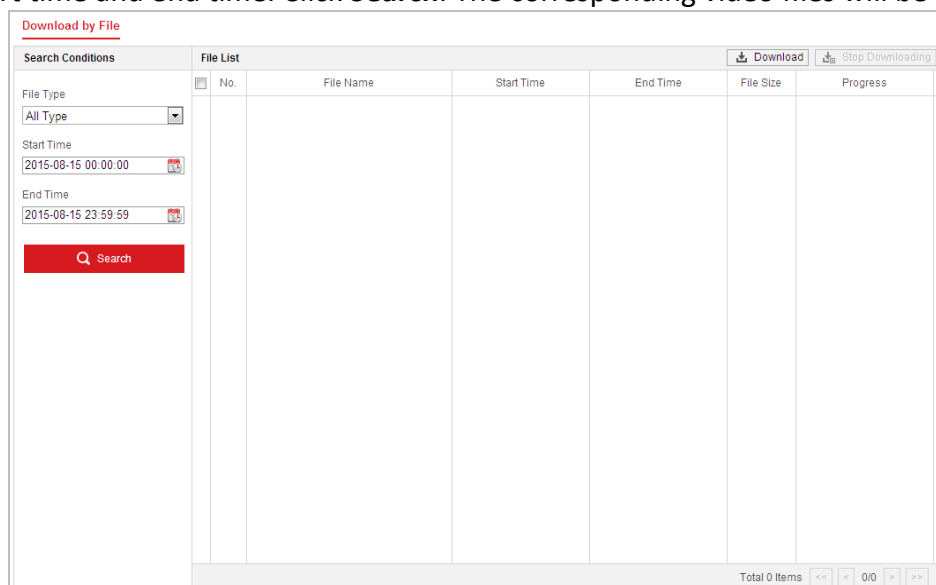


Figure 5-17 Video Downloading interface

3. Check the checkbox in front of the video files that you need to download.
4. Click  **Download** to download the video files.

Notes:

- The progress ratio displays the downloading ratio of the video file.
- You can click Stop to stop the downloading.
- The total number indicates the amount of the video files.
- The video files are not all listed on one page. You can click <<, <, > and >> to turn pages.

5.3.3 Downloading Captured Pictures

Steps:

1. Click  on the playback interface. The download interface pops up.
2. Set the linkage type of capturing the pictures as timing, alarm, motion, etc..
3. Set the start time and end time. Click **Search** and the corresponding picture files will be listed on the left.
4. Check the checkbox in front of the files that you need to download.
5. Click **Download** to download the files.

Chapter 6 Events Settings

Purpose:

This section explains how to configure the camera to respond to alarm events, including motion detection, video tampering, video loss, alarm input, alarm output, exception, and audio exception detection. These events can trigger the alarm actions, such as Send Email, Notify Surveillance Center, Upload to FTP/Memory Card/NAS, etc.

For example, when an external alarm is triggered, the camera sends a notification to an e-mail address.

6.1 Basic Event Configuration

6.1.1 Configuring Motion Detection

Purpose:

Motion detection is a feature which can trigger alarm actions and actions of recording videos when the motion occurred in the surveillance scene.

Steps:

1. Enter the motion detection setting interface:
Configuration > Event > Basic Event > Motion Detection
2. Select the camera **Channel No.** from the dropdown list.

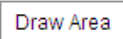
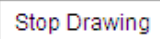
Note:

The Camera 1 is the PTZ channel, and the Camera 2 and Camera 3 are the panoramic view channels.

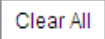
3. Check the **Enable Motion Detection** checkbox to enable this function.
You can check the **Enable Dynamic Analysis for Motion** checkbox if you want the detected object get marked with rectangle in the live view.
4. Select the configuration mode as *Normal* or *Expert* and set the corresponding motion detection parameters.

● **Normal**

Steps:

- (1) Click . Drag the mouse on the live video image to draw a motion detection area.
- (2) Click  to finish drawing.

Notes:

- You can draw up to 8 motion detection areas on the same image.
- You can click  to clear all of the areas.

- (3) Move the slider  to set the sensitivity of the detection.

Channel No. Camera 1

☐ Enable Motion Detection

☐ Enable Dynamic Analysis for Motion

Area Settings | Arming Schedule | Linkage Method

Configuration Normal

Draw Area Clear All

Sensitivity 0

Save

Figure 6-1 Motion Detection Settings-Normal

● Expert

Channel No. Camera 1

☐ Enable Motion Detection

☐ Enable Dynamic Analysis for Motion

Area Settings | Arming Schedule | Linkage Method

Configuration Expert

Draw Area Clear All

Scheduled Image Settings OFF

Area 1

Sensitivity 50

Percentage 0

Save

Figure 6-2 Motion Detection Settings-Expert

Steps:

- (1) Set the **Scheduled Image Settings**, there are OFF, Auto-Switch and Scheduled-Switch selectable. If the switch mode is enabled, you can configure the detection rule for the day and night separately.
OFF: Disable the day and night switch.
Auto-Switch: Switch the day and night mode according to the illumination automatically.

Scheduled-Switch: Switch to the day mode at 6:00 a.m., and switch to the night mode at 18:00 p.m.

- (2) Select **Area** to configure in the dropdown list.
- (3) Set the values of **Sensitivity**.

Sensitivity: The greater the value is, the easier the alarm will be triggered.

5. Set the Arming Schedule for Motion Detection.

- (1) Click **Arming Schedule** tab to enter the arming schedule setting interface.



Figure 6-3 Arming Schedule

- (2) Select the timeline of a certain day, and drag the mouse to set the arming schedule (the start time and end time of the arming task).
- (3) After you set the scheduled task, you can click  and copy the task to other days (optional).

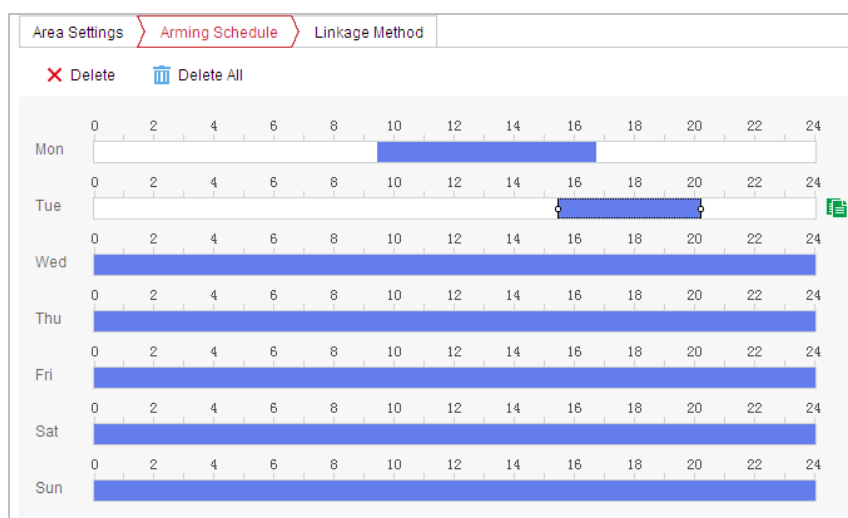


Figure 6-4 Arming Time Schedule

- (4) After setting the arming schedule, you can click a segment to display the segment arming settings interface to edit the segment record parameters (optional).

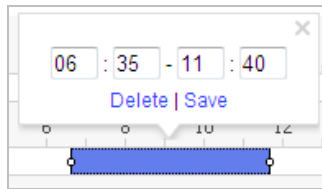


Figure 6-5 Segment Arming Settings

(5) Click  to save the settings.

Note:

The time of each period cannot be overlapped. Up to 8 periods can be configured for each day.

6. Set the Alarm Actions for Motion Detection.

Click  tab to enter the **Linkage Method** interface.

You can specify the linkage method when an event occurs. The following contents are about how to configure the different types of linkage method.

Normal Linkage	Trigger Alarm Output	Trigger Recording
☐ Send Email	☐ A->1	☐ A1
☐ Notify Surveillance Center	☐ A->2	☐ A2
☐ Upload to FTP/Memory Card...		☐ A3

Figure 6-6 Linkage Method

Check the checkbox to select the linkage method. Send Email, Notify Surveillance Center, Upload to FTP/Memory Card/NAS, Trigger Alarm Output and Trigger Recording are selectable.

● **Send Email**

Send an email with alarm information to a user or users when an event occurs.

Note:

- To send the Email when an event occurs, you need to refer to **Section 2.2.2 Advanced Settings - Configuring Email Settings** to set the Email parameters.

● **Notify Surveillance Center**

Send an exception or alarm signal to remote management software when an event occurs.

● **Upload to FTP/Memory Card/NAS**

Capture the image when an alarm is triggered and upload the picture to a FTP server.

Note:

You need a FTP server and set FTP parameters first. Refer to **Section 2.2.2 Advanced Settings - Configuring FTP Settings** for setting FTP parameters.

● Trigger Recording

Record a video when an event occurs.

Note:

You have to set the recording schedule to realize this function. Refer to **Section 5.1 Storage Settings** for settings the recording schedule.

● Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs.

Note:

To trigger an alarm output when an event occurs, refer to **Section 6.1.4 Configuring Alarm Output** to set the alarm output parameters.

6.1.2 Configuring Video Tampering Alarm

Purpose:

You can configure the camera to trigger the alarm actions when the lens is covered.

Steps:

1. Enter the video tampering settings interface:

Configuration > Event > Basic Event > Video Tampering



Figure 6-7 Tampering Alarm

2. Check the **Enable** checkbox to enable the tampering detection.
3. Set the tampering area. Refer to **Step 4** in **Section 6.1.1 Configuring Motion Detection**.
4. Click **Arming Schedule** tab to enter the arming schedule setting interface. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to **Step 5** in **Section 6.1.1 Configuring Motion Detection**.

5. Click **Linkage Method** tab to select the linkage method taken for the video loss alarm. Send Email, Notify Surveillance Center, and Trigger Alarm Output are selectable. Refer to *Step 6* in **Section 6.1.1 Configuring Motion Detection**.
6. Click **Save** to save the settings.

6.1.3 Configuring Alarm Input

Steps:

1. Enter the Alarm Input settings interface:
Configuration > Event > Basic Event > Alarm Input
2. Choose the Alarm Input No. and the Alarm Type. The alarm type can be NO (Normally Open) and NC (Normally Closed).
3. Edit the name in **Alarm Name** (cannot copy) to set a name for the alarm input (optional).

Figure 6-8 Alarm Input Settings

4. Click **Arming Schedule** tab to enter the arming schedule setting interface. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to *Step 5* in **Section 6.1.1 Configuring Motion Detection**.
5. Click **Linkage Method** tab to select the linkage method taken for the video loss alarm. Send Email, Notify Surveillance Center, Upload to FTP/Memory Card/NAS, Trigger Alarm Output and Trigger Recording are selectable. Refer to *Step 6* in **Section 6.1.1 Configuring Motion Detection**.
6. You can also choose the PTZ linking for the alarm input. Check the relative checkbox and select the No. to enable Preset Calling, Patrol Calling or Pattern Calling.
7. You can copy your settings to other alarm inputs.
8. Click **Save** to save the settings.

☐ Normal Linkage ☐ Send Email ☐ Notify Surveillance Center ☐ Upload to FTP	☐ Trigger Alarm Output ☐ A->1 ☐ A->2	☐ Trigger Channel ☐ A1	PTZ Linking ☐ A1 ☐ Preset No. 1 ☐ Patrol No. 1 ☐ Pattern 1
---	---	---	--

Figure 6-9 Linkage Method

6.1.4 Configuring Alarm Output

Steps:

1. Enter the Alarm Output settings interface:
Configuration> Event > Basic Event > Alarm Output
2. Select one alarm output channel in the **Alarm Output** dropdown list.
3. Set a name in (cannot copy) for the alarm output (optional).
4. The **Delay** time can be set to **5sec**, **10sec**, **30sec**, **1min**, **2min**, **5min**, **10min** or **Manual**. The delay time refers to the time duration that the alarm output remains in effect after alarm occurs.
5. Click tab to enter the arming schedule setting interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to *Step 5* in **Section 6.1.1 Configuring Motion Detection**.

Alarm Output No. IP Address
 Delay Alarm Name (cannot copy)
 Alarm Status (cannot copy)

Mon	0 2 4 6 8 10 12 14 16 18 20 22 24
Tue	0 2 4 6 8 10 12 14 16 18 20 22 24
Wed	0 2 4 6 8 10 12 14 16 18 20 22 24
Thu	0 2 4 6 8 10 12 14 16 18 20 22 24
Fri	0 2 4 6 8 10 12 14 16 18 20 22 24
Sat	0 2 4 6 8 10 12 14 16 18 20 22 24
Sun	0 2 4 6 8 10 12 14 16 18 20 22 24

Figure 6-10 Alarm Output Settings

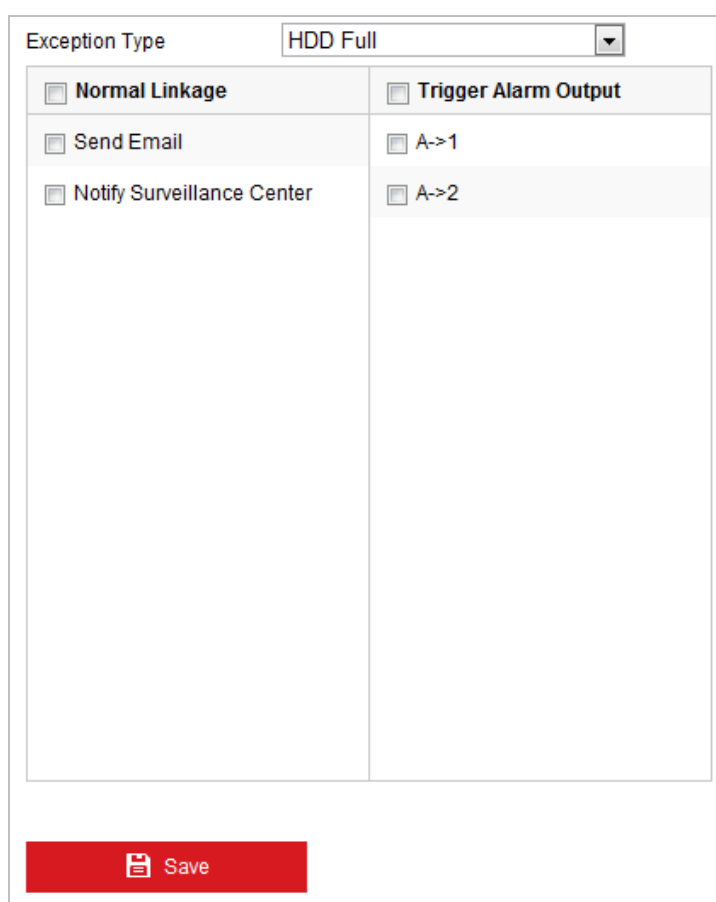
6. You can copy the settings to other alarm outputs.
7. Click  to save the settings.

6.1.5 Handling Exception

The exception type can be HDD full, HDD error, network disconnected, IP address conflicted and illegal login to the cameras.

Steps:

1. Enter the Exception settings interface:
Configuration > Event > Basic Event > Exception
2. Check the checkbox to set the actions taken for the Exception alarm. Refer to *Step 6* in **Section 6.1.1 Configuring Motion Detection**.



Exception Type: HDD Full	
☐ Normal Linkage	☐ Trigger Alarm Output
☐ Send Email	☐ A->1
☐ Notify Surveillance Center	☐ A->2



Figure 6-11 Exception Settings

3. Click  to save the settings.

6.2 Smart Event Configuration

6.2.1 Detecting Audio Exception

Purpose:

When you enable this function and audio exception occurs, the alarm actions will be triggered.

Note:

This function is only supported by certain camera models.

Steps:

1. Enter the audio exception detection interface:

Configuration > Event > Smart Event > Audio Exception Detection

Figure 6-12 Audio Exception Detection

2. Check the **Audio Loss Detection** checkbox to enable the audio input exception detection.
3. Check the **Sudden Increase of Sound Intensity Detection** checkbox to enable the sudden rise detection.
 - **Sensitivity:** Range [1-100], the smaller the value the more severe the sound change will trigger the detection.
 - **Sound Intensity Threshold:** Range [1-100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the actual environment.
4. Check the **Sudden Decrease of Sound Intensity Detection** checkbox to enable the sudden drop detection.

Sensitivity: Range [1-100], the smaller the value the more severe the sound change will trigger the detection.
5. Click **Arming Schedule** tab to enter the arming schedule setting interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to *Step 5* in **Section 6.1.1 Configuring Motion Detection**.
6. Click **Linkage Method** tab to select the linkage method taken for the video loss alarm. Send Email, Notify Surveillance Center, Trigger Alarm Output, and Trigger Recording are selectable. Refer to *Step 3* in **Section 6.1.1 Configuring Motion Detection**.
7. Click **Save** to save the settings.

6.2.2 Configuring Intrusion Detection

Intrusion detection can set an area in the surveillance scene and once the area is entered, a set of alarm action is triggered.

Steps:

1. Enter the intrusion detection interface:
Configuration > Events > Smart Event > Intrusion Detection
2. Check the **Enable** checkbox.

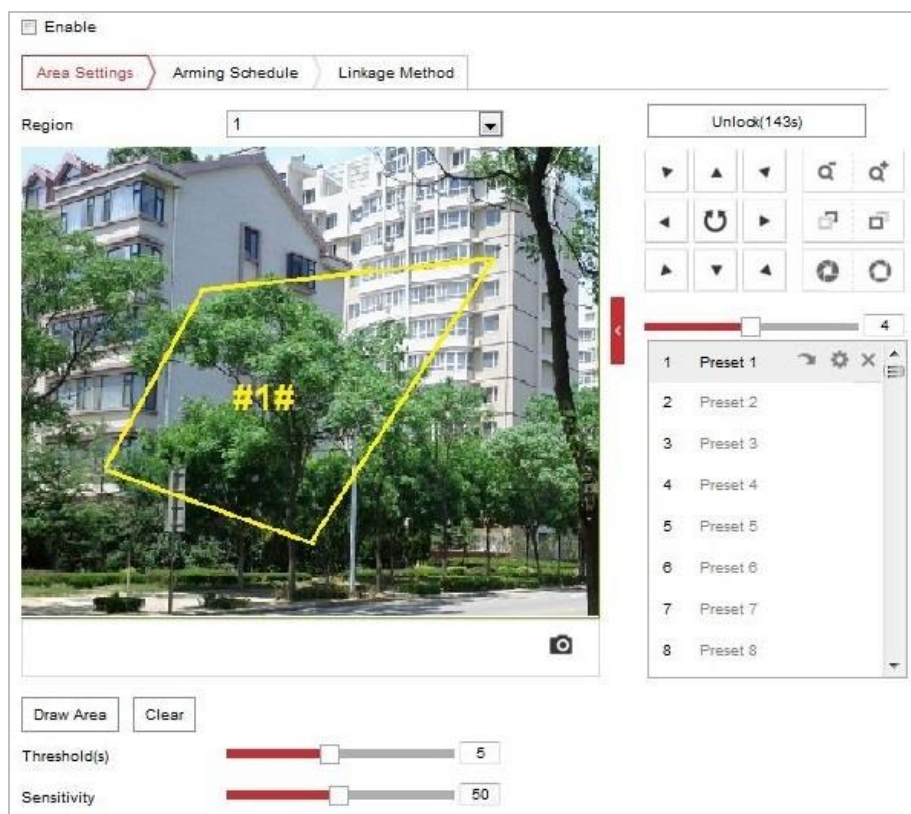


Figure 6-13 Configuring Intrusion Area

3. The event triggered and park action related PTZ movement will be locked for 180 seconds after you enter the intrusion detection interface. Optionally, you can click the **Unlock(69s)** button to manually activate the movement, or lock the movement when the button turns to **Lock** by clicking it.
4. Draw area.
 - (1) Select the Region No.in dropdown list.
 - (2) Click **Draw Area** to draw a rectangle on the image as a defense region.
 - (3) Click on the image to specify a corner of the rectangle, and right-click the mouse after four corners are configured.
5. Configure the parameters for each defense region separately.
 - **Threshold:** Range [0-10s], the threshold for the time of the object loitering in the region. If you set the value as 0, alarm is triggered immediately after the object entering the region.
 - **Sensitivity:** Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.
 - **Detection Target:** Set the detection target. You can select human, vehicle, or all (human &vehicle) as the detection target from the dropdown list. For example, if Human is selected, only human beings will be identified as detection objects.
6. Click **Arming Schedule** tab to enter the arming schedule setting interface. The time schedule

configuration is the same as the settings of the arming schedule for motion detection. Refer to *Step 5* in **Section 6.1.1 Configuring Motion Detection**.

7. Click **Linkage Method** tab to select the linkage method taken for intrusion detection, Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Alarm Output and Trigger Recording are selectable. Refer to *Step 3* in **Section 6.1.1 Configuring Motion Detection**.
8. Click **Save** to save the settings.

6.2.3 Configuring Line Crossing Detection

The virtual plane detection can be adopted for the intrusion detection. Once the virtual plane is detected being traversed according to the configured direction, a set of alarm action is triggered.

Steps:

1. Enter the Line Crossing Detection interface:
Configuration > Event > Smart Event > Line Crossing Detection
2. Check the **Enable** checkbox to enable the line crossing detection function.
3. Select the Line in dropdown list to configure.
4. The event triggered and park action related PTZ movement will be locked for 180 seconds after you enter the line crossing detection interface. Optionally, you can click the **Unlock(69s)** button to manually activate the movement, or lock the movement when the button turns to **Lock** by clicking it.

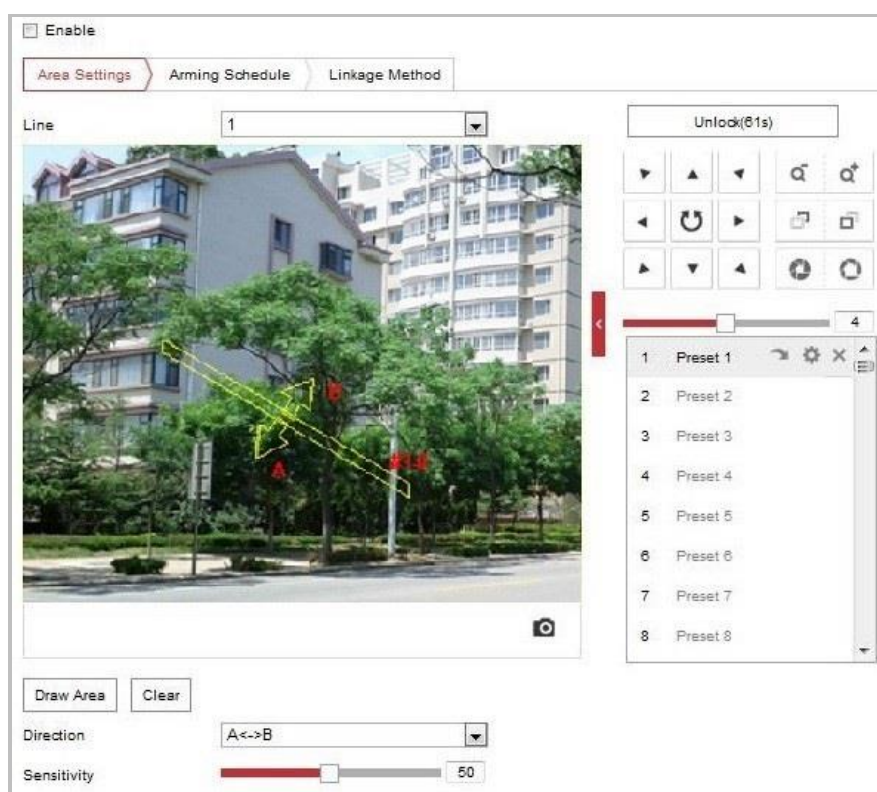


Figure 6-14 Configuring Line

5. Draw area.
 - (1) Click **Draw Area** to draw a line on the image.
 - (2) Click the line to switch to the editing mode.
Drag an end to the desired place to adjust the length and angle of the line. And drag the line to adjust the location.
6. Configure the parameters for each defense region separately.
 - **Direction:** Select the detection direction in the dropdown list, there are A<->B, A->B and B->A

selectable.

- **Sensitivity:** Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.
 - **Detection Target:** Set the detection target. You can select human, vehicle, or all (human & vehicle) as the detection target from the dropdown list. For example, if Human is selected, only human beings will be identified as detection objects.
7. Click **Arming Schedule** tab to enter the arming schedule setting interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to *Step 5* in **Section 6.1.1 Configuring Motion Detection**.
 8. Click **Linkage Method** tab to select the linkage method taken for the line crossing detection, Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Alarm Output and Trigger Recording are selectable. Refer to *Step 3* in **Section 6.1.1 Configuring Motion Detection**.
 9. Click **Save** to save the settings.

6.2.4 Configuring Region Entrance Detection

Purpose:

Region entrance detection function detects people, vehicle or other objects which enter a pre-defined virtual region from the outside place, and some certain actions can be taken when the alarm is triggered.

Steps:

1. Enter the Region Entrance Detection settings interface:
Configuration> Event > Smart Event> Region Entrance Detection
2. Check the checkbox of **Enable** to enable the Region Entrance Detection function.

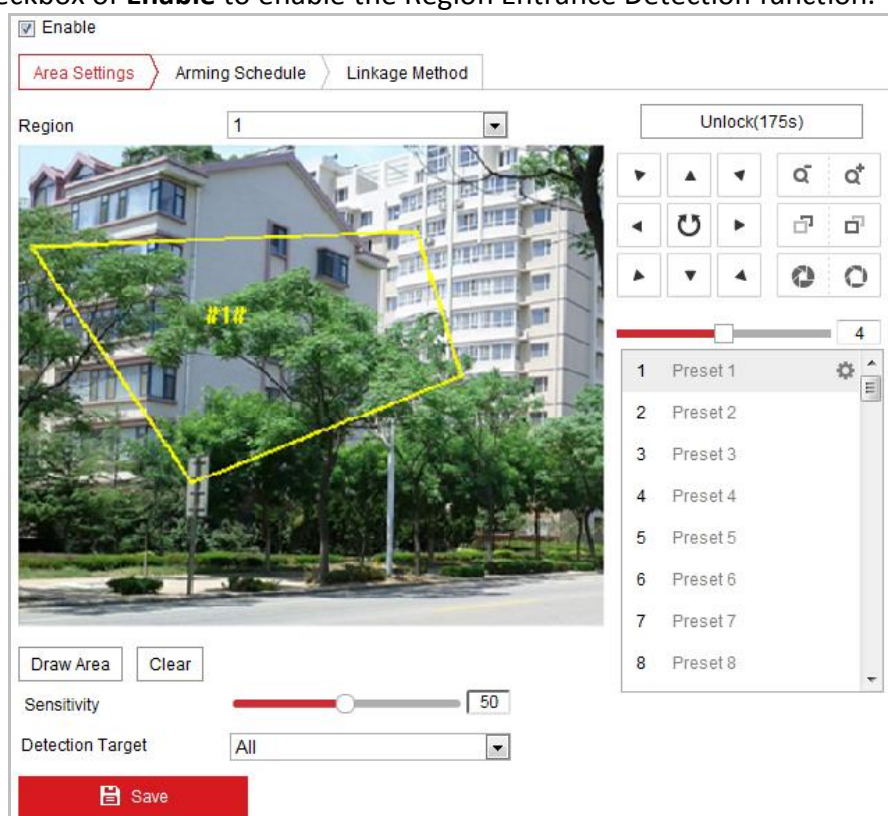


Figure 6-15 Configuring Region Entrance Detection

3. Select the region from the dropdown list for detection settings.
4. Click the **Draw Area** button to start the region drawing.

- Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.

Repeat the step to configure other regions. You can click the  button to clear all pre-defined regions.

Sensitivity: Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.

Detection Target: Set the detection target for the region entrance detection. You can select human, vehicle, or all (human & vehicle) as the detection target from the dropdown list. If Human is selected, only human beings will be identified as detection objects and as well as Vehicle.

- Click  tab to enter the arming schedule setting interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to *Step 5* in **Section 6.1.1 Configuring Motion Detection**.
- Click  tab to select the linkage method taken for the video loss alarm, Notify surveillance center, send email, upload to FTP, trigger channel, smart tracking and trigger alarm output are selectable. Refer to *Step 3* in **Section 6.1.1 Configuring Motion Detection**.
- Click  to save the settings.

6.2.5 Configuring Region Exiting Detection

Purpose:

Region exiting detection function detects people, vehicle or other objects which exit from a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

Steps:

- Enter the Region Exiting Detection settings interface:
Configuration > Event > Smart Event > Region Exiting Detection
- Check the checkbox of **Enable** to enable the Region Exiting Detection function.

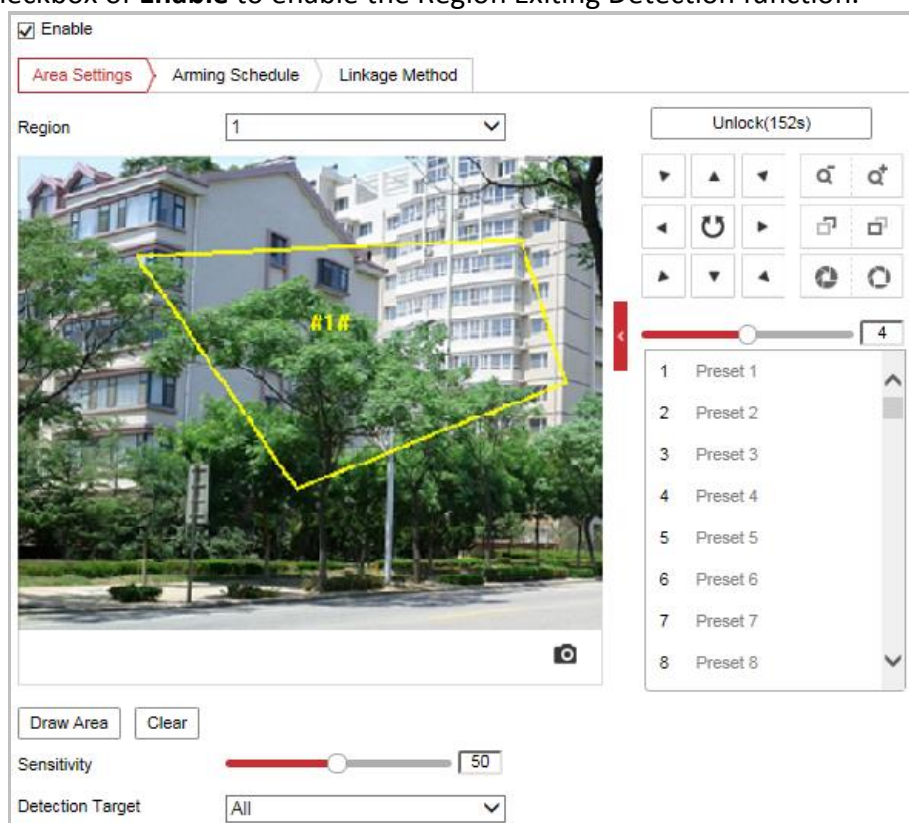


Figure 6-16 Configuring Region Exiting Detection

- Select the region from the dropdown list for detection settings.

4. Click the Draw Area button to start the region drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.

Repeat the step to configure other regions. Up to 4 regions can be set. You can click the Clear button to clear all pre-defined regions.

Sensitivity: Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.

Detection Target: Set the detection target for the region entrance detection. You can select human, vehicle, or all (human & vehicle) as the detection target from the dropdown list. If Human is selected, only human beings will be identified as detection objects and as well as Vehicle.

6. Click Arming Schedule tab to enter the arming schedule setting interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to *Step 5* in **Section 6.1.1 Configuring Motion Detection**.
7. Click Linkage Method tab to select the linkage method taken for the video loss alarm, Notify surveillance center, send email, upload to FTP, trigger channel, smart tracking and trigger alarm output are selectable. Refer to *Step 3* in **Section 6.1.1 Configuring Motion Detection**.
8. Click Save button to save the settings.

6.2.6 Configuring Unattended Baggage Detection

Purpose:

Unattended baggage detection function detects baggage which is left in a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

Steps:

1. Enter the Unattended Baggage Detection settings interface:
Configuration> Event > Smart Event> Unattended Baggage Detection
2. Check the checkbox of **Enable** to enable the Unattended Baggage Detection function.

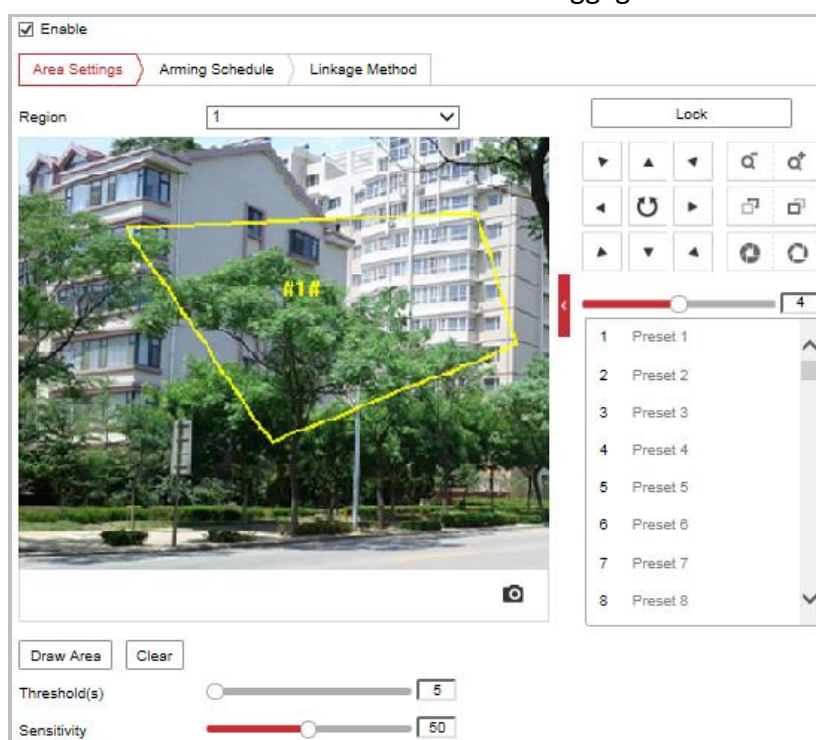
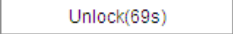
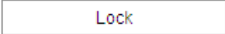
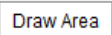
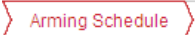


Figure 6-17 Configuring Unattended Baggage Detection

3. The event triggered and park action related PTZ movement will be locked for 180 seconds after you enter the unattended baggage detection interface. Optionally, you can click the  button to manually activate the movement, or lock the movement when the button turns to  by clicking it.
4. Select the region from the dropdown list for detection settings.
5. Click the  button to start the region drawing.
6. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.

Repeat the step to configure other regions. Up to 4 regions can be set. You can click the  button to clear all pre-defined regions.
7. Configure the parameters for each defense region separately.
 - **Threshold Level:** If you set the value as 5, alarm is triggered immediately after the object entering the region.
 - **Sensitivity Level:** The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.
8. Click  tab to enter the arming schedule setting interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to **Section 6.1.1 Configuring Motion Detection** for more details.
9. Click  tab to select the linkage method taken for the unattended baggage alarm, Notify surveillance center, send email, upload to FTP, trigger channel, smart tracking and trigger alarm output are selectable. Refer to **Section 6.1.1 Configuring Motion Detection** for more details.
10. Click  button to save the settings.

6.2.7 Configuring Object Removal Detection

Purpose:

Object removal detection function detects objects which remove in a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

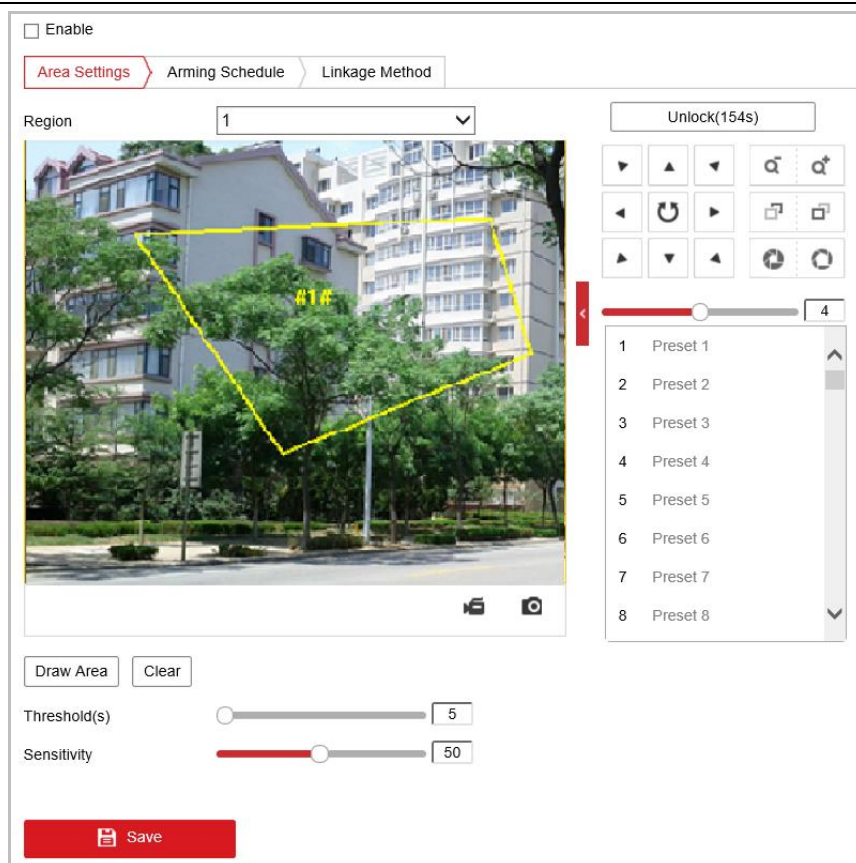


Figure 6-18 Configuring Object Removal Detection

Steps:

1. Enter the Object Removal Detection settings interface:
Configuration > Event > Smart Event > Object Removal Detection
2. Check the checkbox of **Enable** to enable the Object Removal Detection function.
3. The event triggered and park action related PTZ movement will be locked for 180 seconds after you enter the unattended baggage detection interface. Optionally, you can click the Unlock(69s) button to manually activate the movement, or lock the movement when the button turns to Lock by clicking it.
4. Select the region from the dropdown list for detection settings.
5. Click the Draw Area button to start the region drawing.
6. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing. Repeat the step to configure other regions. Up to 4 regions can be set. You can click the Clear button to clear all pre-defined regions.
7. Configure the parameters for each defense region separately.
 - **Threshold Level:** If you set the value as 5, alarm is triggered immediately after the object entering the region.
 - **Sensitivity Level:** The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.
8. Click Arming Schedule tab to enter the arming schedule setting interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to **Section 6.1.1 Configuring Motion Detection** for more details.

9. Click **Linkage Method** tab to select the linkage method taken for the object removal alarm, Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel, Smart Tracking and Trigger Alarm Output are selectable. Refer to **Section 6.1.1 Configuring Motion Detection** for more details.

Click **Save** button to save the settings.

6.3 Behavior Analysis

Purpose:

Multiple rules can be configured for different requirements to do intelligent analysis.

Note:

Behavior analysis is only available for panoramic camera channel. If the camera supports more than one panoramic channel, select a channel and start configuration.

6.3.1 Configuring Overlay & Capture

Steps:

1. Enter the Behavior Analysis configuration interface:
Configuration > Behavior Analysis > Overlay & Capture

Figure 6-19 Overlay & Capture

2. Set the display information:
 - Display VCA info. on Stream: The green frames will be displayed on the target if in a live view or playback.
 - Display Target info. on Alarm Picture: There will be a frame on the target on the uploaded alarm picture if the checkbox is checked.
 - Display Rule info. on Alarm Picture: The captured target and the configured area will be framed on the alarm picture.

3. Set the Snapshot:

- You can check the checkbox to upload JPEG image to surveillance center when VCA alarm occurs.
- You can also set the quality of the picture.

4. Click to save the settings.

6.3.2 Shield Region

Purpose:

Shield Region is the user-defined areas in surveillance scene that the analysis doesn't take effect. Usually, they can be privacy areas. Set if needed.

Steps:

1. Click **Shield Region** tab to enter the shield region configuration interface
2. Click **Draw Area**. Draw area by left click end-points in the live view window, and right click to finish the area drawing. Polygon area with up to 10 sides are supported.
3. Click **Save** to save the settings.

6.3.3 Rule Configuration

This section provides detailed configuration steps for each rule.

1. Click Rule Tab to enter the rule configuration interface.
2. Check the checkbox in Rule List to enable the rule for behavior analysis.
3. For the selected rule, set the Rule Name, Rule Type, and complete rule-specified settings.

● **Line Crossing**

Purpose:

This function can be used for detecting people, vehicles and objects traversing a set virtual plane. The traversing direction can be set as bidirectional, from left to right or from right to left. The alarm will be triggered if the rule is broken.

Steps:

- 1) Create new rule: Click  add a new rule.
- 2) Select rule type: Click the dropdown list and select **Line Crossing** as the rule type.

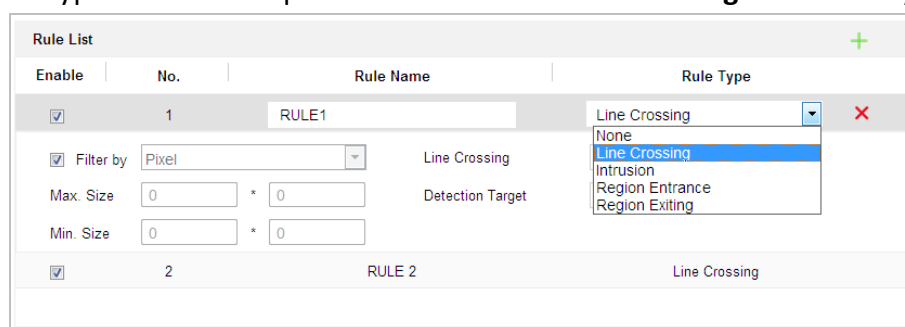


Figure 6-20 Select Rule Type

3) Configure the rule area:

Click  on the tool bar of the live view panel. Adjust the position and length of the line on the live view panel.



Figure 6-21 Draw Line

- 4) Click the dropdown list in the rule list to select the crossing direction.

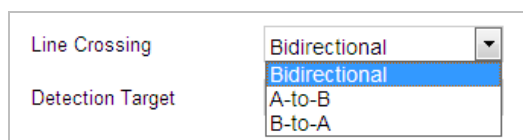


Figure 6-22 Select Crossing Direction

- 5) Enable rules: Check the **Enable** checkbox of each rule in the rule list to enable the rule.

- 6) Click  Save to save the settings.

● Intrusion

Purpose:

This function can be used for detecting whether there are people, vehicles and objects intrude into the pre-defined region longer than the set duration. The alarm will be triggered if the rule is broken.

Steps:

- 1) Create new rule: Click  add a new rule.
- 2) Select rule type: Click the dropdown list and select **Intrusion** as the rule type.

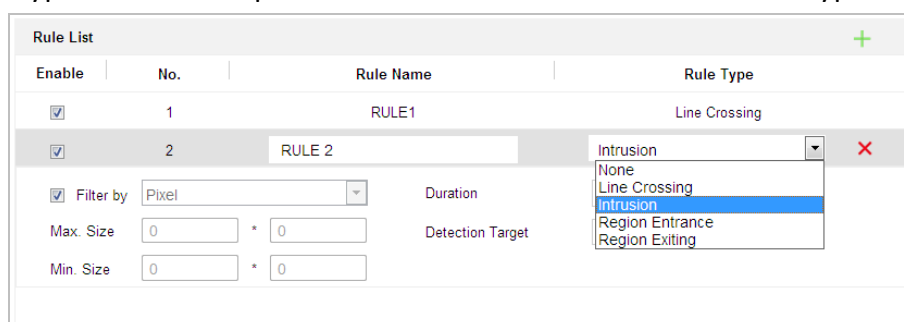


Figure 6-23 Select Rule Type

- 3) Configure the rule area:

Click  on the tool bar of the live view panel. Click the mouse on the live view panel. Right click the mouse to finish drawing.



Figure 6-24 Draw Area

- 4) Set the duration from 1 to 100.
- 5) Enable rules: Check the **Enable** checkbox of each rule in the rule list to enable the rule.
- 6) Click  Save to save the settings.

● Region Entrance

Purpose:

This function can be used for detecting people, vehicles and objects entering the pre-defined region. The alarm will be triggered if the rule is broken.

Steps:

- 1) Create new rule: Click  to add a new rule.
- 2) Select rule type: Click the dropdown list and select **Region Entrance** as the rule type.

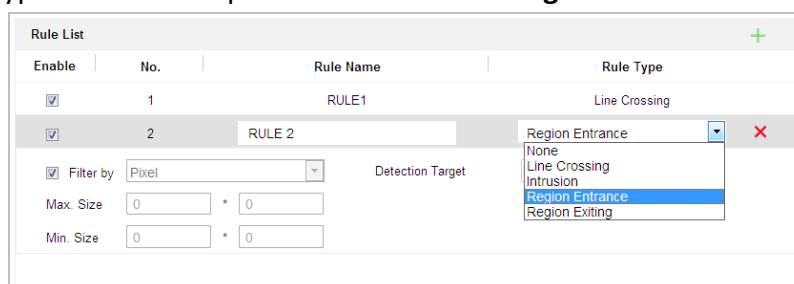


Figure 6-25 Select Rule Type

- 3) Configure the rule area:

Click  on the tool bar of the live view panel. Click the mouse on the live view panel. Right click the mouse to finish drawing.

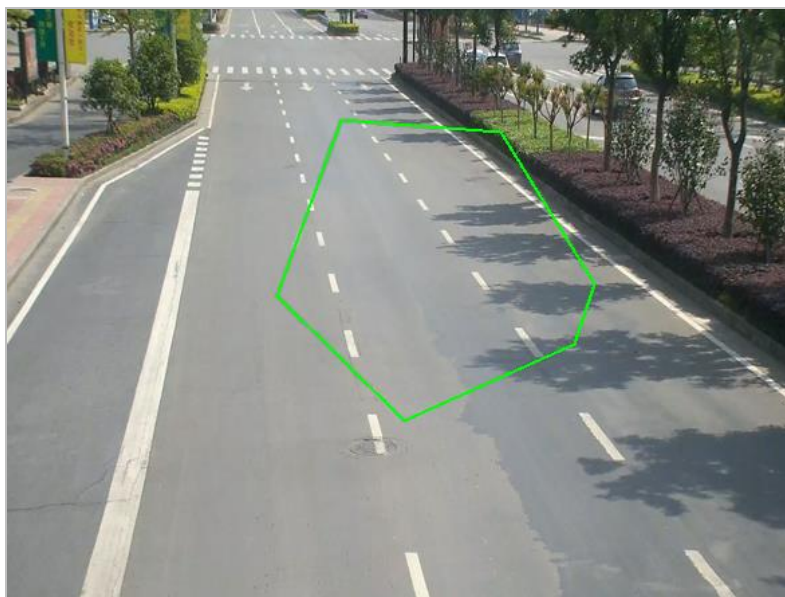


Figure 6-26 Draw Area

4) Enable rules: Check the **Enable** checkbox of each rule in the rule list to enable the rule.

5) Click  Save to save the settings.

● Region Exiting

Purpose:

This function can be used for detecting people, vehicles and objects exiting the pre-defined region. The alarm will be triggered if the rule is broken.

Steps:

- 1) Create new rule: Click  to add a new rule.
- 2) Select rule type: Click the dropdown list and select **Region Exiting** as the rule type.

Rule List 			
Enable	No.	Rule Name	Rule Type
☒	1	RULE1	Line Crossing
☒	2	RULE 2	Region Exiting None Line Crossing Intrusion Region Entrance Region Exiting

☒ Filter by Pixel ▼

Detection Target

Max. Size *

Min. Size *

Figure 6-27 Select Rule Type

3) Configure the rule area:

Click  on the tool bar of the live view panel. Click the mouse on the live view panel. Right click the mouse to finish drawing.

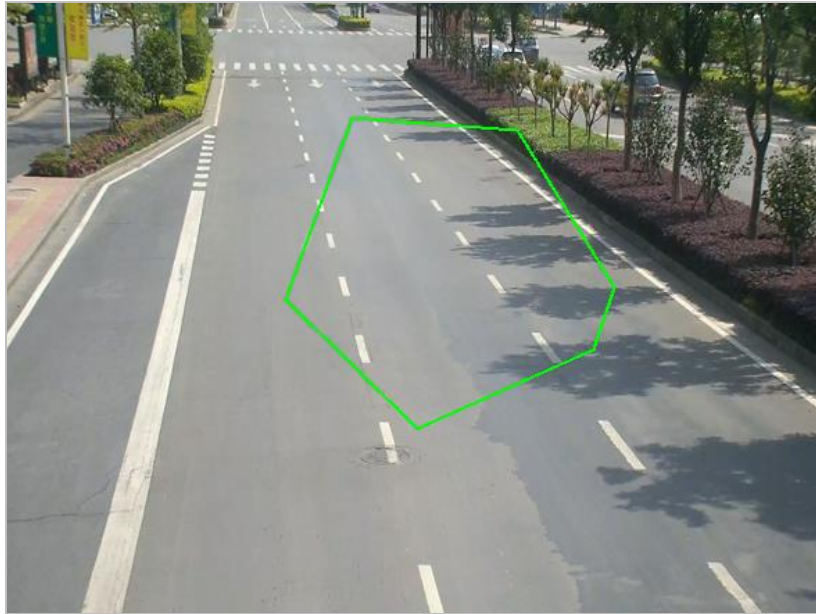


Figure 6-28 Draw Area

- 4) Enable rules: Check the **Enable** checkbox of each rule in the rule list to enable the rule.
- 5) Click  Save to save the settings.
4. Click **Save** to save the settings.
5. Click  **Arming Schedule** tab to enter the arming schedule setting interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to *Step 5* in **Section 6.1.1 Configuring Motion Detection**.
6. Click  **Linkage Method** tab to select the linkage method taken for the video loss alarm, Notify surveillance center, send email, upload to FTP, trigger channel, smart tracking and trigger alarm output are selectable. Refer to *Step 3* in **Section 6.1.1 Configuring Motion Detection**.
7. Click  Save button to save the settings.

6.3.4 Advanced Configuration

Purpose:

The following contents are about how to configure the parameters of behavior analysis algorithm.

Steps:

1. Enter the Advanced Configuration interface:
Configuration > Behavior Analysis > Advanced Configuration
2. Adjust Parameters.
Restart VCA: Click **Restart** to restart the VCA function.
3. Global Size Filter
Global Size filter is valid for all panoramic channels. Targets larger or smaller than the set size range are filtered out.

Steps:

- 1) Enable Global Size Filter.
- 2) Click  and draw a max size frame on live image.
- 3) Click  and draw a min size frame on live image.

4) Click Save to save the settings.

4. Click  to save the settings.

6.4 Face Capture

Face capture function detects and captures faces in surveillance scenes. When the grading of the detected face exceeds an algorithm-defined value, the PTZ camera channel captures the face and triggers linkage actions. Set up Capture Parameters and advanced parameters before using the function.

Notes:

- When adjusting image and video effect, you can click  to capture a image and click  to record a video clip for testing. Pictures and videos are saved in your local computer.
- Face capture function detects and captures faces in surveillance scenes. When the grading of the detected face exceeds an algorithm-defined value, the PTZ camera channel captures the face and triggers linkage actions. Set up Overlay & Capture, Rule and Advanced Configuration before using the function.
- For certain camera models, you need to select Face Capture on VCA Resource page first: **Configuration > System > System Settings**
- Face capture is only supported by certain camera models.

6.4.1 Overlay & Capture

Purpose:

You can choose to configure Display on Stream, Display on Picture, Snapshot Settings, Camera Information, and Text Overlay on stream/picture.

Enter the Overlay & Capture configuration interface:

Configuration > Face Capture > Overlay & Capture

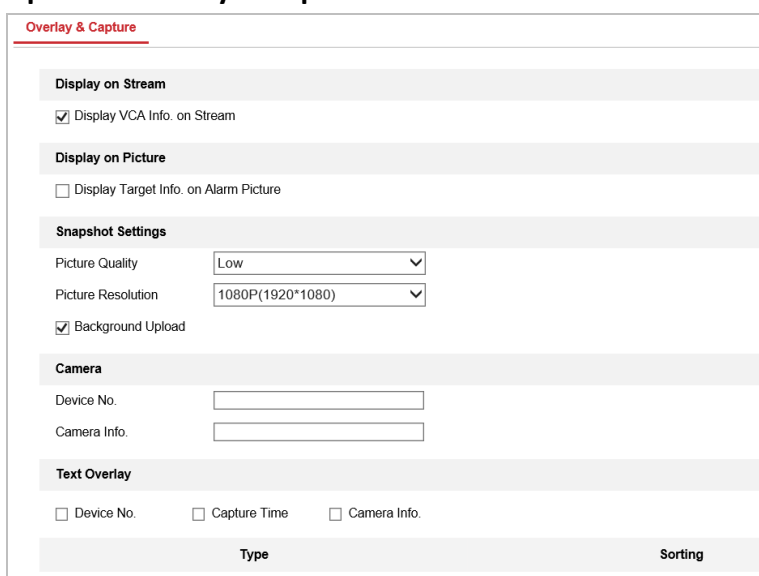


Figure 6-29 Overlay & Capture interface

- **Display on Stream:** Check the checkbox, then the green frames will be displayed on the target if in a live view or playback.

- **Display on Picture:** Check the checkbox, then there will be a frame on the target on the uploaded alarm picture if the checkbox is checked.
- **Snapshot Settings:** You can set the quality and resolution for the captured picture.
- **Picture Quality** from the dropdown list. High, Medium, and Low are selectable.
 - ◆ Select **Picture Quality and Picture Resolution** from the dropdown list.
 - ◆ Check **Background Upload** to upload the background image.

Note:

Background upload is only available for face capture camera.

- **Camera Information:** Enter Device No. and Camera Info.
- **Text Overlay:** Check Device No., Capture Time, and Camera Info, and these camera information can be overlaid on captured picture. You can check desired items and adjust their order to display on captured pictures by clicking the up arrow or down arrow.

Text Overlay	
☒ Device No.	☒ Capture Time ☒ Camera Info.
Type	Sorting
Camera Info.	↑ ↓
Capture Time	↑ ↓
Device No.	↑ ↓

Figure 6-30 Picture Overlay Information

6.4.2 Rule

Steps:

1. Check **Enable** to enable the function.
2. Click **Area Settings** to set up face capture rule.

Rule

☒ Enable

Area Settings

Patrol Schedule

Linkage Method

Detection Scene Detection Scene 1

Min. Pupil Distance

41

✓

Mounting Height

4.5

m

Unlock(88s)

↶

↷

↶

↷

↶

↷

↶

↷

↶

↷

↶

↷

↶

↷

↶

↷

1 Preset 1

2 Preset 2

3 Preset 3

4 Preset 4

5 Preset 5

6 Preset 6

7 Preset 7

8 Preset 8

Save

Figure 6-31 Area Settings

- (1) Select a **Detection Scene** from the dropdown list.
 - (2) Adjust the live image to a desired scene. you can use PTZ control panel or click  to locate a scene with a face. Click **Lock** to lock PTZ for further settings.
 - (3) Click  and draw detection area on live image.
 - (4) Click  and draw **Min. Pupil Distance** on live image.
 - (5) Input **Mounting Height** of the camera.
 - (6) Save the settings for the detection scene.
 - (7) Repeat the steps to set other detection scenes.
 - (8) Save the settings
3. Click  to enable camera patrols the detection scenes following configured order and dwell time, and capture faces during its patrol.

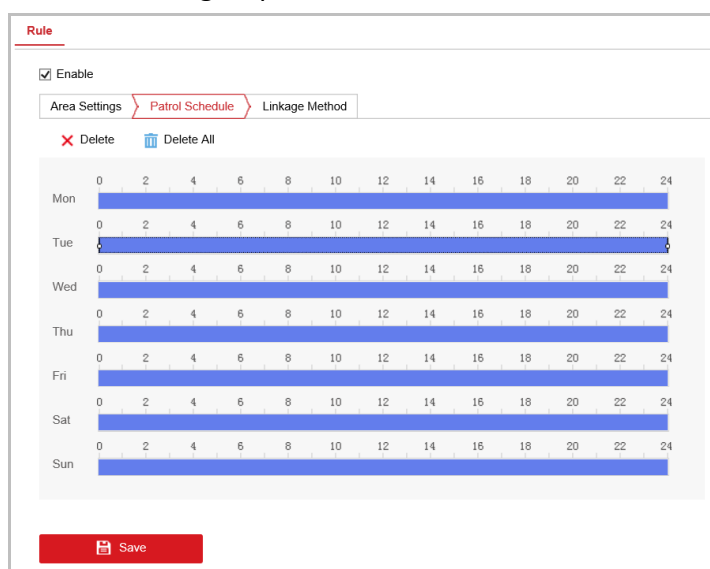


Figure 6-32 Patrol Schedule

- (1) Click the set blue time bar.
 - (2) Click **Configuration** in the pop-up bubble.
 - (3) Add detection scenes, adjust the patrol sequence and set dwell time for each detection scene.
 - (4) Save the settings by clicking **OK**.
 - (5) You can copy the settings of a day to other days by click  on right end of the time bar.
4. Click  to set linkage method. Refer to **Section 6.1.1 Configuring Motion Detection** for detailed configuration.

6.4.3 Advanced Configuration

Purpose:

The following contents are about how to configure the parameters of face capture algorithm.

Note:

Face Capture Version shows current algorithm version, which cannot be edited.

Figure 6-33 Advanced Face Capture Parameters

Following parameters can be configured on this interface:

- **Generation Speed:** The speed to identify a target can be set by adjusting the slider, ranging from 1 to 5. The higher the value is, the faster the target will be recognized. The default value is recommended.
- **Sensitivity:** The sensitivity to identify a target can be set by adjusting the slider, ranging from 1 to 5. The higher the value is, the easier a face will be detected, and the higher possibility of misinformation would be. The default value of 3 is recommended.
- **Face Capture Mode:** Best Shot and Quick Shot are available.
 - ◆ **Best Shot** stands for the best picture after the target leaving the detection area.
 - **Capture Times:** Refers to the capture times a face will be captured during its stay in the detection area.
 - **Capture Interval:** The frame interval to capture a picture. If you set the value as 1(default), it means the camera captures the face in every frame.
 - **Capture Threshold:** It stands for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.
 - ◆ **Quick Shot:** You can define quick shot threshold and max. capture interval.
 - **Quick Shot Threshold:** It stands for the quality of face to trigger quick shot.
 - ◆ **Face Exposure:** Check the checkbox to enable the Face Exposure. The device automatically adjusts exposure level when human faces appear in the scene.
 - **Reference Brightness:** The reference brightness of a face in the face exposure mode. If a face in the actual scene is brighter than the set reference brightness, the device lower the exposure level. If a face in the actual scene is darker than the set reference, the device increases the exposure level.
 - **Minimum Duration:** The extra time the device keeps the face exposure level after the face disappears in the scene.
 - ◆ **Face Filtering Time:** It means the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.

Restore Default: Click  to restore all the settings in advanced configuration to the factory default.

6.5 People Density

This function can detect the level of people density in the configured area.

6.5.1 Rule

Purpose:

Set up detection areas, density levels and linkage method on this page.

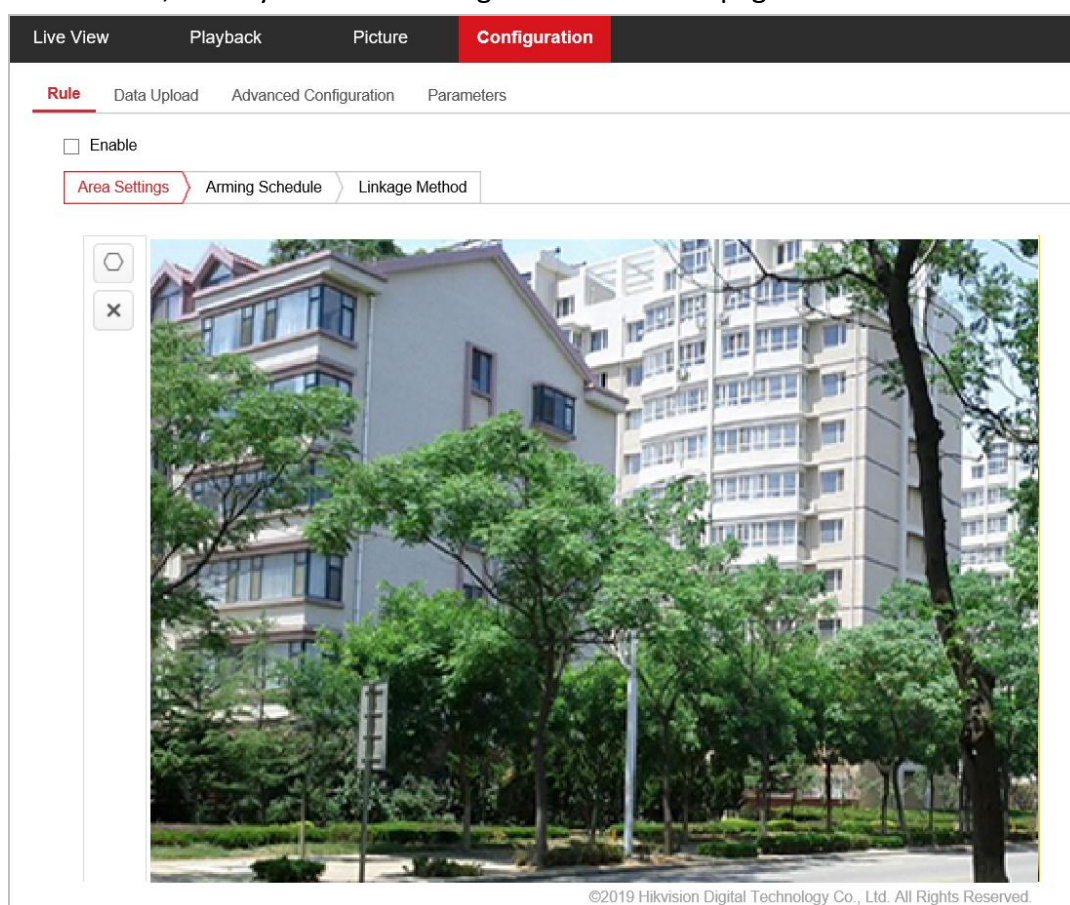


Figure 6-34 People Density Rule configuration

Steps:

1. Click  and draw detection area on live image. Click  to clear all the areas.

Note:

You can set 8 areas at most, and the area can be set as polygon of 10 sides at most.

2. Set target size as Large-size Target (40*40 pixel) or Small-size Target (20*20 pixel) for each detection area from the dropdown list.

Note:

Click  or , a frame of 40*40 pixel or 20*20 pixel will be showed on live picture. Choose the corresponding target size by comparing the target size with frame size.

- Set Density Level, including Number of People. Three levels can be configured in total, and the density increases from level 1 to level 3.

Note:

The number you input means the lower limit of each level. For example, set the Number of People of Level 1 as 10, Level 2 is 100, and level 3 is 1000. When the number of people in the detection area is less than 10, the alarm will not be triggered. When the number of people is between 10 and 100, Level 1 alarm will be triggered. When the number of people is between 100 and 1000, Level 2 alarm will be triggered. When the number is above 1000, Level 3 alarm will be triggered.

- Click  to save the settings.
- Set the **Arming Schedule**.
 - Check **Enable** to edit the arming schedule.
 - Select the timeline of a certain day, and drag the left button of the mouse to set the capture schedule (the start time and end time of the recording task).
 - (Optional) After you set the scheduled task, you can click  and copy the task to other days.
 - Click Save to save the schedule.
- Set the **Linkage Method** for People Density detection.

Note:

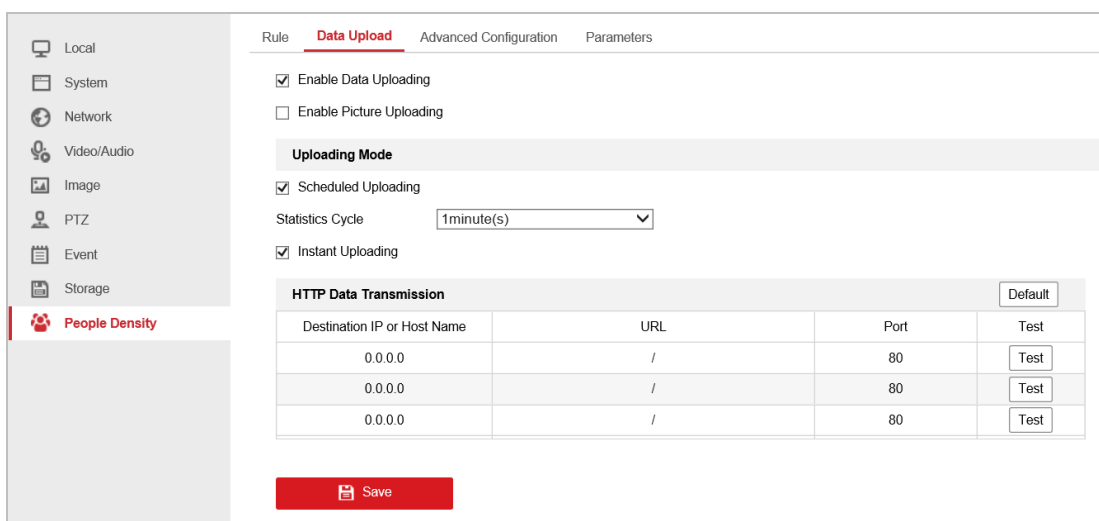
Before you start, make sure the **Data Uploading** function has been enabled. Go to Configuration > People Density > Data Upload to check the **Enable Data Uploading** checkbox.

The alarm actions will be triggered when the number of people surpass the setting value in surveillance scene.

- Check **Enable** to enable the function. Notify Surveillance Center is selectable.
Notify Surveillance Center: Send an exception or alarm signal to remote management software when an event occurs.
- Click Save to save the settings.

6.5.2 Data Upload

Configure the content and mode when upload to surveillance center.



The screenshot shows the 'Data Upload' configuration page. On the left is a sidebar with navigation options: Local, System, Network, Video/Audio, Image, PTZ, Event, Storage, and People Density (selected). The main area has tabs: Rule, Data Upload (active), Advanced Configuration, and Parameters. Under 'Data Upload', there are checkboxes for 'Enable Data Uploading' (checked) and 'Enable Picture Uploading' (unchecked). Below is the 'Uploading Mode' section with 'Scheduled Uploading' (checked) and 'Instant Uploading' (checked). The 'Statistics Cycle' is set to '1minute(s)'. The 'HTTP Data Transmission' section includes a table with columns: Destination IP or Host Name, URL, Port, and Test. The table has three rows, all with '0.0.0.0' in the first column and '/' in the second. The 'Port' column has '80' in the first two rows and '80' in the third. Each row has a 'Test' button. A 'Default' button is at the top right of the table. At the bottom of the page is a red 'Save' button.

Destination IP or Host Name	URL	Port	Test
0.0.0.0	/	80	<button>Test</button>
0.0.0.0	/	80	<button>Test</button>
0.0.0.0	/	80	<button>Test</button>

Figure 6-35 Configure Data Upload

Steps:

1. Check **Enable Data Uploading** checkbox, and the data of people density detection will be uploaded to surveillance center.
2. Check **Enable Picture Uploading** checkbox, the alarm will be uploaded to surveillance center with pictures.
3. Set Uploading Mode. Scheduled Uploading and Instant Uploading are selectable.
 - **Scheduled Uploading:** The detection data and pictures can be uploaded to surveillance center at certain time interval.
Check **Scheduled Uploading** checkbox to enable the function, and select a **Statistics Cycle** from the dropdown list.
 - **Instant Uploading:** Once the level of people density changes, the detection data and pictures will be uploaded to surveillance center immediately.
Check Instant Uploading checkbox to enable the function.
4. Configure HTTP Data Transmission. Input IP address, URL and Port, then click Test to test if it succeeds.
5. Click **Save** to save the settings.

6.5.3 Advanced Configuration

Configure the overlay information displayed on live image.

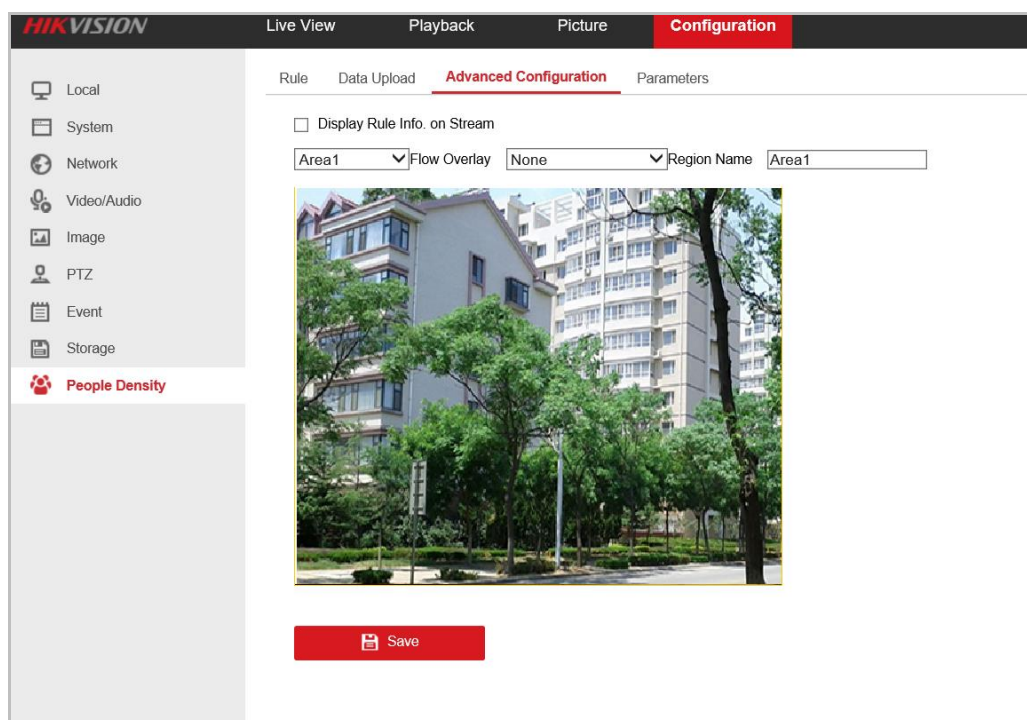


Figure 6-36 Advanced Configuration

Steps:

1. Check **Display Rule Info. on Stream** to enable this function.
2. Choose **Flow Overlay** from the dropdown list, None, Level, Number of People, and Number of People/Level are selectable.
3. Edit Region Name for every detection area you set before.
4. Click **Save** to save the settings.

6.5.4 Parameters

Check the version of people gathering density algorithms library on this page.

6.6 Smart Display

Click Smart Display to display captured pictures in face capture function.

Note:

The function requires the support of camera and certain web browser. Adjust your browser settings according to the pop-up notification.

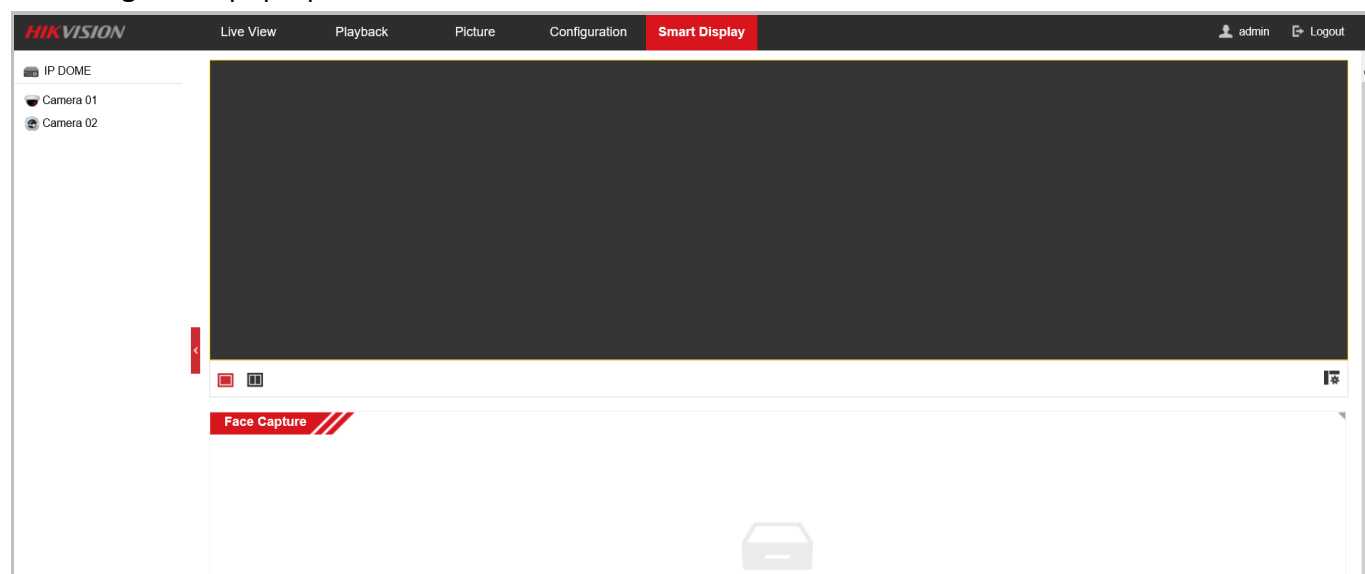


Figure 6-37 Smart Display Interface

The layout and information to show are configurable. Click  to show the configuration page.

Chapter 7 System Settings

7.1 Basic Information

7.1.1 Viewing Basic Information

Enter the **Basic Information** interface:

Configuration > System > System Settings > Basic Information

In the **Basic Information** interface, you can edit the Device Name and Device No.

Other information of the camera, such as Model, Serial No., Firmware Version, Encoding Version, Web Version, Plugin Version, Number of Channels, Number of HDDs, Number of Alarm Input and Number of Alarm Output are displayed. The information cannot be changed in this menu. It is the reference for maintenance or modification in future.

Basic Information	Time Settings	RS485	DST
Device Name	IP DOME		
Device No.	88		
Model	XX-XxxXxxx-X		
Serial No.	XX-XxxXxxx-XxxxXXXXXXXX		
Firmware Version	VX.X.X build XxxXXXX		
Encoding Version	VX.X build XxxXXXX		
Web Version	VX.X.X build XxxXXXX		
Plugin Version	VX.X.X.XX		
Number of Channels	1		
Number of HDDs	0		
Number of Alarm Input	7		
Number of Alarm Output	2		

Figure 7-1 Device Information

7.1.2 Time Settings

Purpose:

You can follow the instructions in this section to configure the time which can be displayed on the video. There are Time Zone, Time Synchronization, Daylight Saving Time (DST) functions for setting the time. Time Synchronization consists of auto mode by Network Time Protocol (NTP) server and manual mode. To enter the Time settings interface:

Configuration > System > System Settings > Time Settings

Figure 7-2 Time Settings

◆ Configuring Time Synchronization by NTP Server

Steps:

- (1) Check the radio button to enable the **NTP** function.
- (2) Configure the following settings:

Server Address: IP address of NTP server.

NTP Port: Port of NTP server.

Interval: The time interval between the two synchronizing actions by NTP server. It can be set from 1 to 10080 minutes.

Figure 7-3 Time Sync by NTP Server

- (3) You can click  to check whether the configuration is succeeded.

Note:

If the camera is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the camera is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.

◆ Configuring Time Synchronization Manually

Steps:

- (1) Check the **Manual Time Sync** radio button.
- (2) Click  to set the system time from the pop-up calendar.
- (3) Click  to save the settings.

Note:

You can also check the **Sync. with computer time** checkbox to synchronize the time of the camera with the time of your computer.

Figure 7-4 Time Sync Manually

◆ Select the Time Zone

Purpose:

When the camera is taken to another time zone, you can use the **Time Zone** function to adjust the time. The time will be adjusted according to the original time and the time difference between the two time zones.

From the **Time Zone** dropdown menu as shown in Figure 7-5, select the Time Zone in which the camera locates.

Figure 7-5 Time Zone Settings

7.1.3 Configuring RS-485

Purpose:

The RS-485 serial port is used to control the PTZ of the camera. The configuring of the PTZ parameters should be done before you control the PTZ unit.

Steps:

1. Enter RS-485 Port setting interface:

Configuration > System > System Settings > RS-485

Figure 7-6 RS-485 Settings

2. Set the RS-485 parameters and click  to save the settings.

Note:

The Baud rate, PTZ Protocol and PTZ Address parameters of the camera should be exactly the same as those of the control device.

7.1.4 Configuring DST (Daylight Saving Time)

Purpose:

If there is the habit of adjusting clocks forward in your country in certain time period of a year, you can turn this function on. The time will be adjusted automatically when the Daylight Saving Time (DST) comes.

Steps:

1. Enter the DST settings interface:
Configuration > System > System Settings > DST
2. Check ☐ **Enable DST** to enable the DST function.
3. Set the date of the DST period.
4. Click  to save the settings.

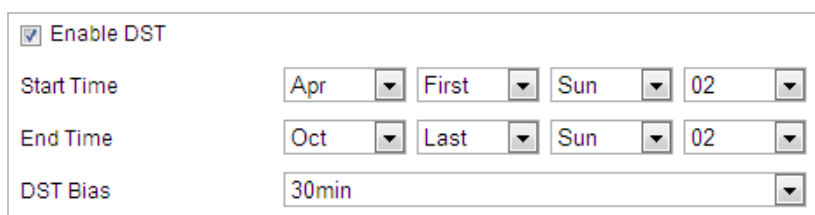


Figure 7-7 DST Settings

7.1.5 VCA Resource

VCA resource offers users options to enable certain VCA function and disable others when several VCA functions are available. It helps allocate more resources to the wanted functions.

Steps:

1. Enter the VCA Resource interface: **Configuration > System settings > VCA Resource**
2. Select the desired VCA option.
3. Save the settings. A reboot is needed for the settings to take effect.

Note:

The function may not be supported by some camera models.

7.1.6 Image Stitching

Purpose:

Set Image Stitching parameters for panoramic channel on this page.

Steps:

4. Enter the Image Stitching interface: **Configuration > System settings > Image Stitching**

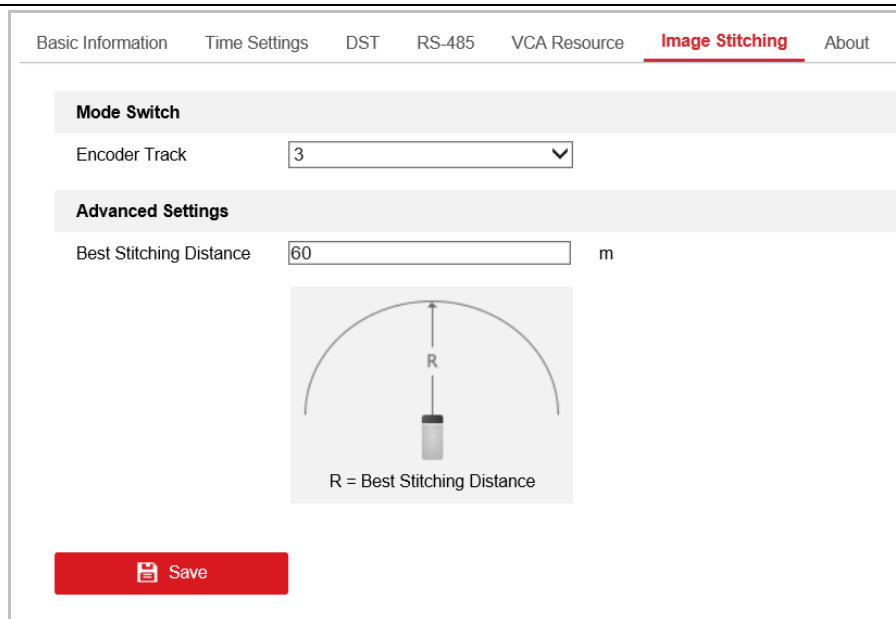


Figure 7-8 Image Stitching Interface

5. Configure the following settings:

- **Encoder Track:** Stream can be divided into several tracks in order to make up for the deficiency of decoder. 1 track and 3 tracks are selectable, and it is recommended to select 3, when the decoder is in poor performance.

Note:

Only the main stream of 2400W and 1600W panorama camera support this function.

- **Best Stitching Distance:** You can set the distance between the lens and the stitching surface for the best stitching image quality. The further the distance is, the worse the stitching image quality is.

For example, if you set the best stitching distance as 30 meters, the stitching image of 30 meters far from the lens is the best quality. The stitching image of 20 or 40 meters far from the lens is not good and the image of 10 or 50 meters far from the lens is the worst.

7.1.7 Open Source Software

Configuration > System settings > About

Click **View License**, you can check Open Source Software Licenses.

7.2 Maintenance

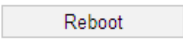
7.2.1 Upgrade & Maintenance

● Rebooting the Camera

Steps:

1. Enter the Maintenance interface:

Configuration > System > Maintenance > Upgrade & Maintenance:

2. Click  to remotely reboot the camera.

● Restoring Default Settings

Steps:

1. Enter the Maintenance interface:
Configuration > System > Maintenance > Upgrade & Maintenance:
2. Click or to restore the default settings.

Note:

Clicking button will restore all the parameters to default settings including the IP address and user information. Use this button with caution.

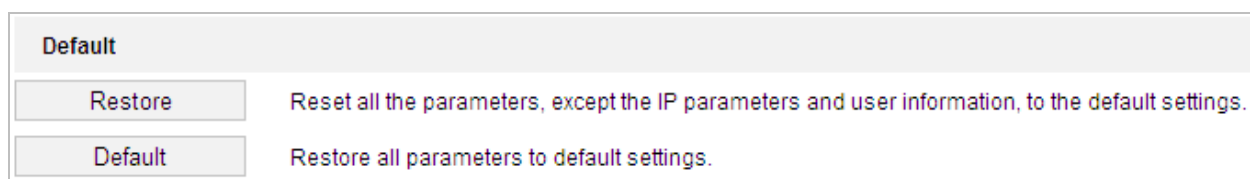


Figure 7-9 Restore Default Settings

● Exporting Configuration File

Steps:

1. Enter the Maintenance interface:
Configuration > System > Maintenance > Upgrade & Maintenance
2. Click to select the directory as the saving path to start exporting configuration file.

● Importing Configuration File

Steps:

1. Enter the Maintenance interface:
Configuration > System > Maintenance > Upgrade & Maintenance
2. Click to select the local configuration file and then click to start importing configuration file.

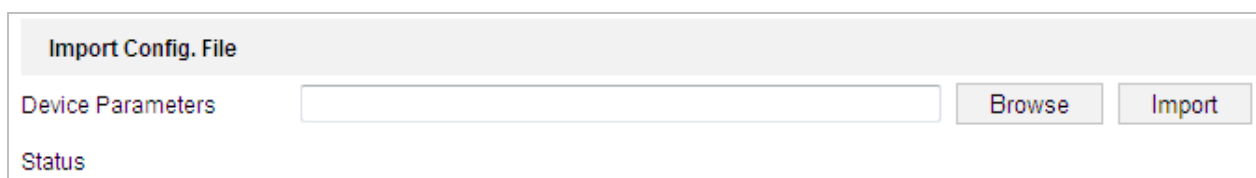


Figure 7-10 Import Configuration File

Note:

You need to reboot the camera after importing configuration file.

● Upgrading the System

Steps:

1. Enter the Upgrade & Maintenance interface:
Configuration > System > Maintenance > Upgrade & Maintenance
2. Select Firmware or Firmware Directory.

- **Firmware:** when you select **Firmware**, you need to find the firmware in your computer to upgrade the device.
- **Firmware Directory:** You need to find the directory where the firmware locates. The device can find the firmware in the directory automatically.

3. Click **Browse** to select the local upgrade file and then click **Upgrade** to start remote upgrade.

Note:

The upgrading process will take 1 to 10 minutes. Do not disconnect the power of the camera during the upgrading process. The camera reboots automatically after upgrading.



Figure 7-11 Remote Upgrade

7.2.2 Log Searching

Purpose:

The operation, alarm, exception and information of the camera can be stored in log files. You can also export the log files on your demand.

Before you start:

Configure network storage for the camera or insert a memory card in the camera.

Steps:

1. Enter the Log interface:

Configuration > System > Maintenance > Log

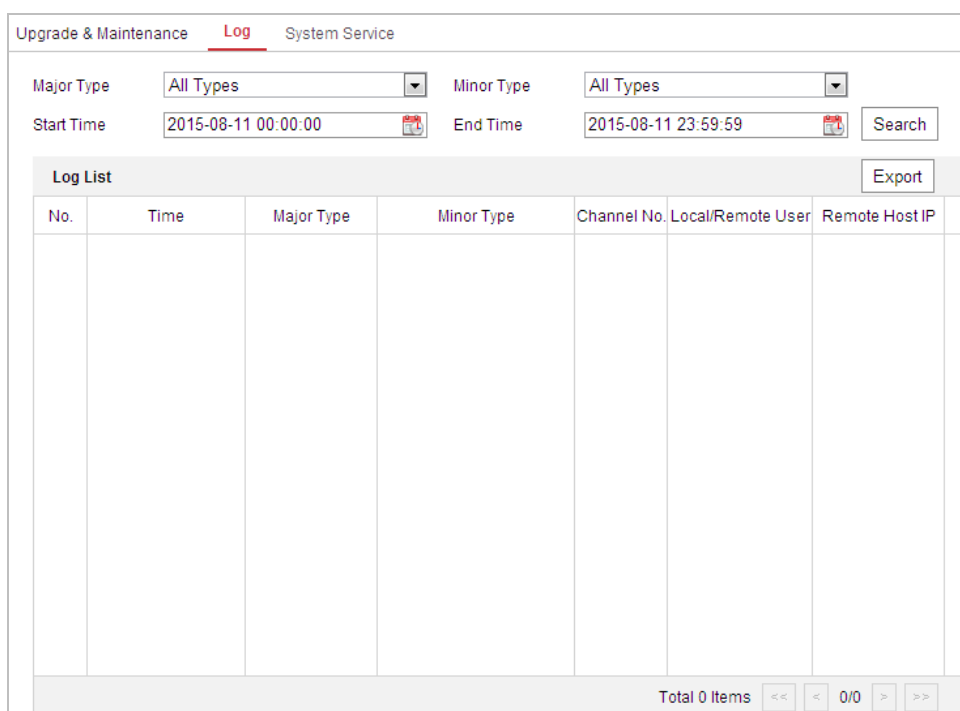


Figure 7-12 Log Searching Interface

2. Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time as shown in Figure 7-12.
3. Click  to search log files. The matched log files will be displayed on the **Log List**.
4. To export the log files, click **Save Log** to save the log files in your computer.

7.2.3 System Service

Hardware

It refers to the hardware service, for example supplement light, the camera supports. Check correspondent function to enable it. Supported functions varies according to the different cameras.

Note:

The supplement light configuration is only supported by certain models.

Software

- **Display camera range of the PTZ channel**

Check the function, the view of the PTZ channel is marked on the panoramic view with a rectangle. It helps locate the PTZ camera in the whole scenes.

- **Live View Connection**

You can set the maximum live view connection to control the simultaneous visits.

Note:

The number of live view connection varies according to different camera models. The maximum number of live view connection equals the number of camera channels multiplied by 6. If the camera supports 2 channels, up to 12 users are supported for live view at the same time.

Steps:

1. Enter the interface of configuring the remote connection:

Configuration > System > Maintenance > System Service

2. Input a number in text field as the upper limit of the remote connection number. E.g. when you specify the remote connection number as 10, then the 11th remote connection cannot be established.



Figure 7-13 Live View Connection Settings

3. Click  to activate the settings.

7.3 Security

7.3.1 Configuring Authentication

Purpose:

You can specifically secure the stream data of live view. RTSP authentication and WEB authentication are supported.

Steps:

1. Enter the Authentication interface:
Configuration > System > Security > Authentication
2. Select the authentication type. Digest is the recommended safer authentication way.
3. Click  to save the settings.

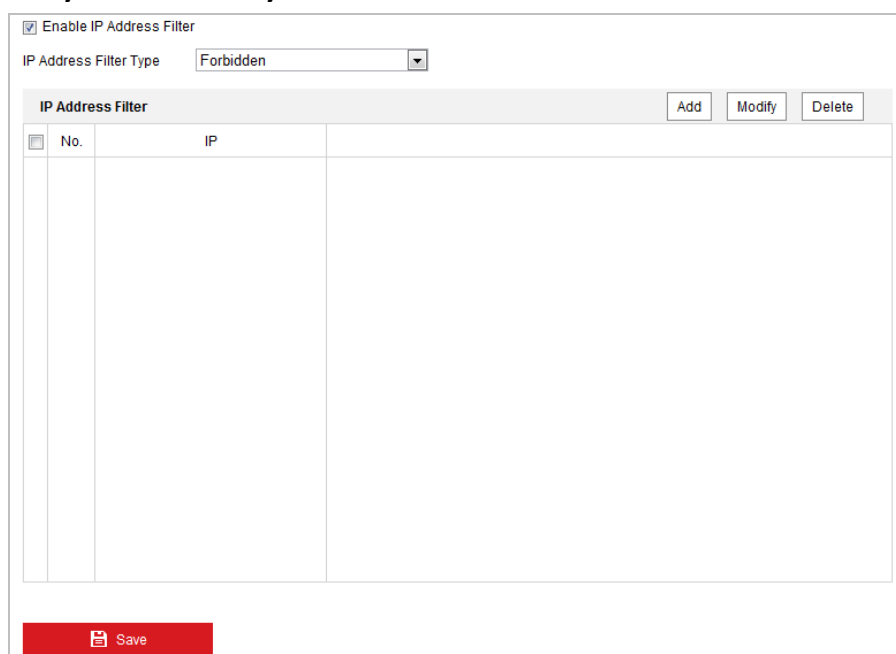
7.3.2 Configuring IP Address Filter

Purpose:

With this function on, the camera allows certain IP addresses whether to log in or not.

Steps:

1. Enter IP Address Filter interface:
Configuration > System > Security > IP Address Filter



☒ Enable IP Address Filter

IP Address Filter Type: Forbidden

IP Address Filter		Add	Modify	Delete
No.	IP			



Figure 7-14 IP Address Filter

2. Check the **Enable IP Address Filter** checkbox.
3. Select the type of IP Address Filter in the dropdown list, Forbidden and Allowed are selectable.
4. Set the IP Address Filter list.
 - Add an IP Address

Steps:

- (1) Click **Add** to add an IP.
- (2) Input the IP Address.

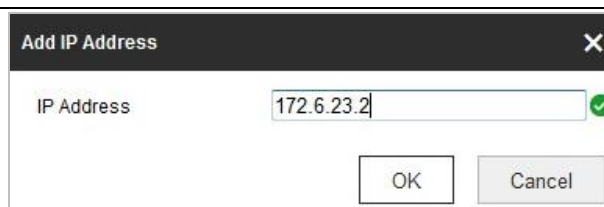


Figure 7-15 Add an IP

(3) Click **OK** to finish adding.

- Modify an IP Address

Steps:

(1) Left-click an IP address from filter list and click **Modify**.

(2) Modify the IP address in the text filed.

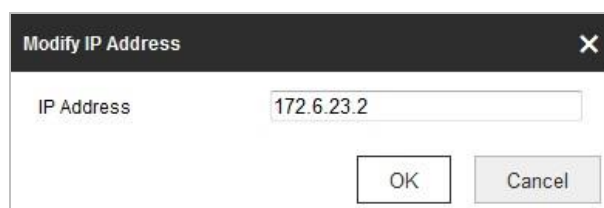


Figure 7-16 Modify an IP

(3) Click **OK** to finish modifying.

- Delete an IP Address

Left-click an IP address from filter list and click **Delete**.

- Delete all IP Addresses

Click **Clear** to delete all the IP addresses.

5. Click **Save** to save the settings.

7.3.3 Configuring Security Service

Steps:

1. Enter the Security Service interface:
Configuration > System > Security > Security Service
2. Check the **Enable Illegal Login Lock** checkbox to automatically lock the device IP after performing 5 failed password attempts.

7.4 User Management

Enter the User Management interface:

Configuration > System > User Management

- **As Administrator**

Administrator need to input correct admin password when changing settings of other operators or users.

- **As Operator or User**

- **Password Recommendation**

Online User

Configuration > System > User Management > Online Users

User List					Refresh
No.	User Name	Level	IP Address	User Operation Time	
1	admin	Administrator	10.15.2.15	2017-11-14 14:59:15	

You can see the current users who are visiting the device through this interface. User information, such as user name, level, IP address, and operation time, is displayed in the User List. Click **Refresh** to refresh the list.

Appendix

Appendix 1 SADP Software Introduction

◆ Description of SADP

SADP (Search Active Devices Protocol) is a kind of user-friendly and installation-free online device search tool. It searches the active online devices within your subnet and displays the information of the devices. You can also modify the basic network information of the devices using this software.

◆ Search active devices online

● Search online devices automatically

After launch the SADP software, it automatically searches the online devices every 15 seconds from the subnet where your computer locates. It displays the total number and information of the searched devices in the Online Devices interface. Device information including the device type, IP address and port number, etc. will be displayed.

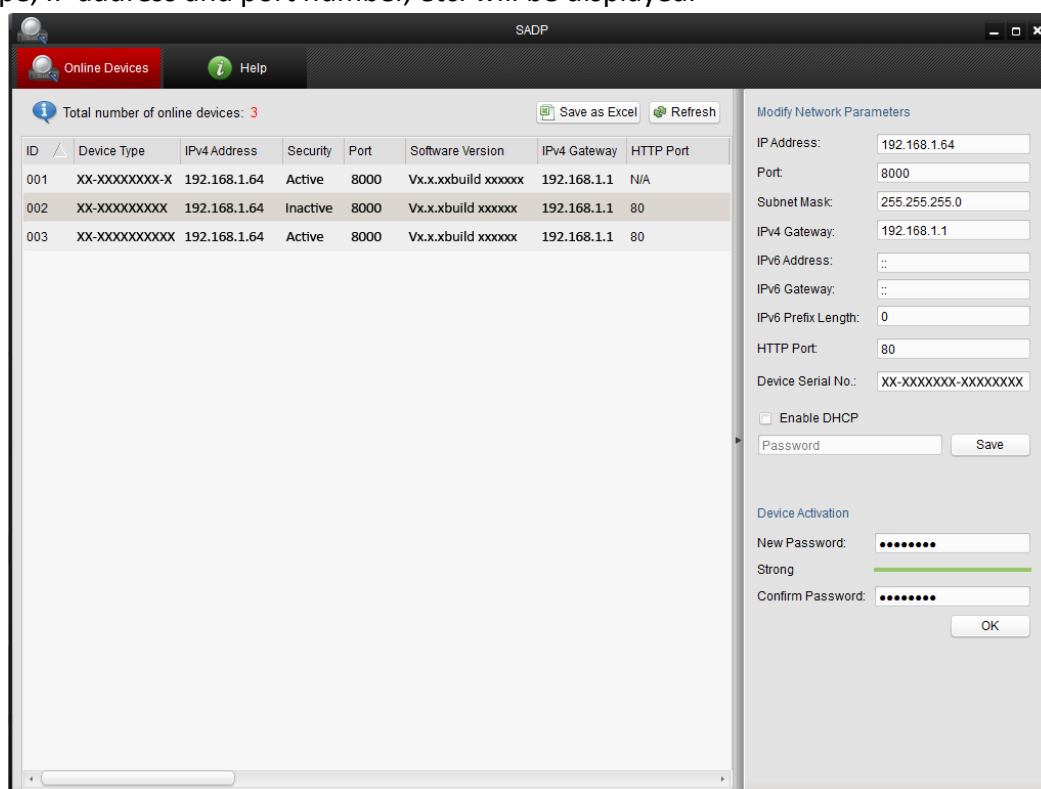
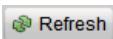


Figure A.1.1 Searching Online Devices

Note:

Device can be searched and displayed in the list in 15 seconds after it went online; it will be removed from the list in 45 seconds after it went offline.

● Search online devices manually

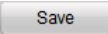
You can also click  to refresh the online device list manually. The newly searched devices will be added to the list.

Note:

You can click  or  on each column heading to order the information; you can click  to expand the device table and hide the network parameter panel on the right side, or click  to show the network parameter panel.

◆ Modify network parameters

Steps:

1. Select the device to be modified in the device list and the network parameters of the device will be displayed in the **Modify Network Parameters** panel on the right side.
2. Edit the modifiable network parameters, e.g. IP address and port number.
3. Enter the password of the admin account of the device in the **Password** field and click  to save the changes.



- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

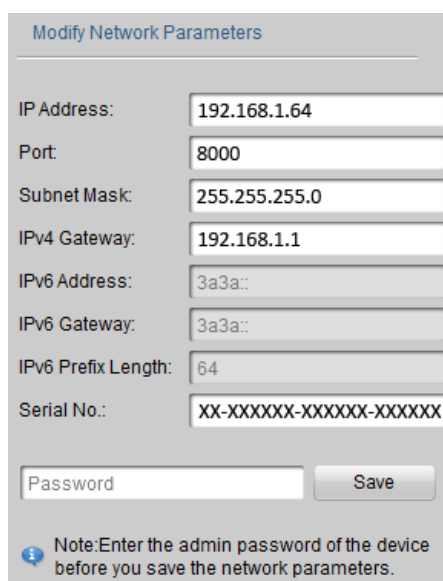


Figure A.1.2 Modify Network Parameters

Appendix 2 Statics, Interference Lightning and Surge Protection

This product adopts TVS plate lightning protection technology to avoid damage caused by pulse signal that is below 3000V, like instantaneous lighting stroke, surging, etc. According to the actual outdoor situation, necessary protection measures must be taken, besides ensuring the electrical safety.

- The distance between signal transmission wires and High-voltage equipment or high-voltage cable is at least 50m.
- Outdoor wiring should better be routed under eaves as much as possible.
- In the open field, wiring should be buried underground in sealed steel pipe, and the steel-pipe should be one-point grounding. Overhead routing method is forbidden.
- In strong thunderstorm area or high induction voltage areas (such as high-voltage transformer substation), high power lightning protection apparatus and lightning conductor are necessary to be added.
- The design of lightning protection and grounding of the outdoor devices and cables should be considered together with the lightning protection demand of buildings. It also must conform to the related national standards and industrial standards.
- The system should be equipotential grounded. The grounding equipment must conform to the demands of system anti-jamming and electrical safety both and it must not appear short circuit or mixed circuit with the zero conductor of strong grid. When the system is grounded alone, the resistance should be no more than 4Ω . The sectional area of the grounding cable should be no less than 25mm^2 . For grounding instructions, refer to the Installation Manual of Camera.

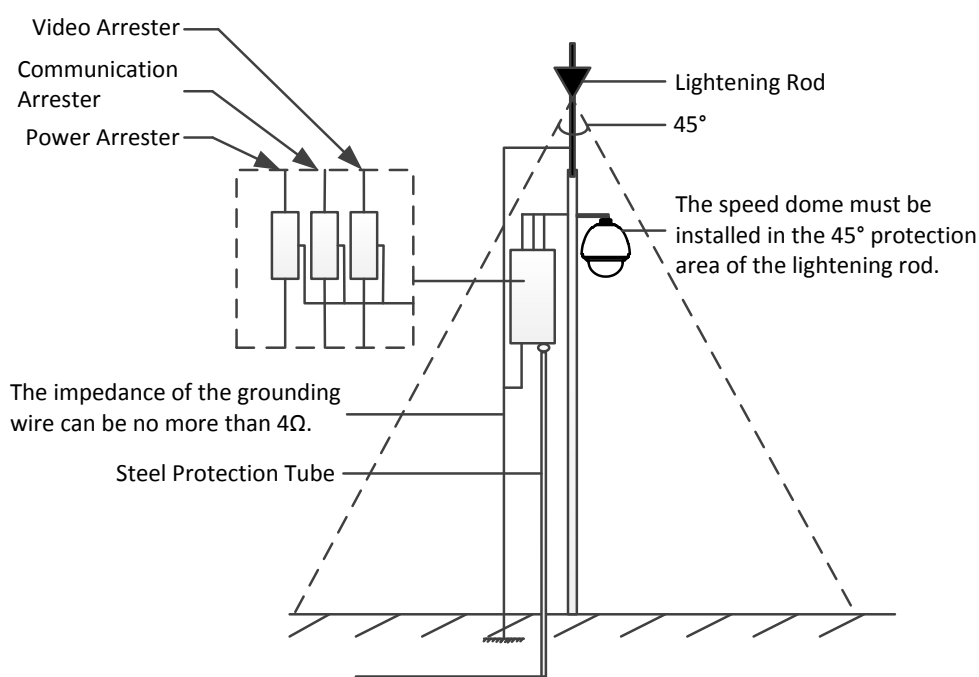


Figure A.3.1 Lightning & Surge Protection

Grounding for Cement Pole/Wall Installation:

When the camera is installed in environment where is relatively insulating to the earth, e.g., cement pole or cement wall, then only the control center requires proper grounded locally. Refer to the following figure.

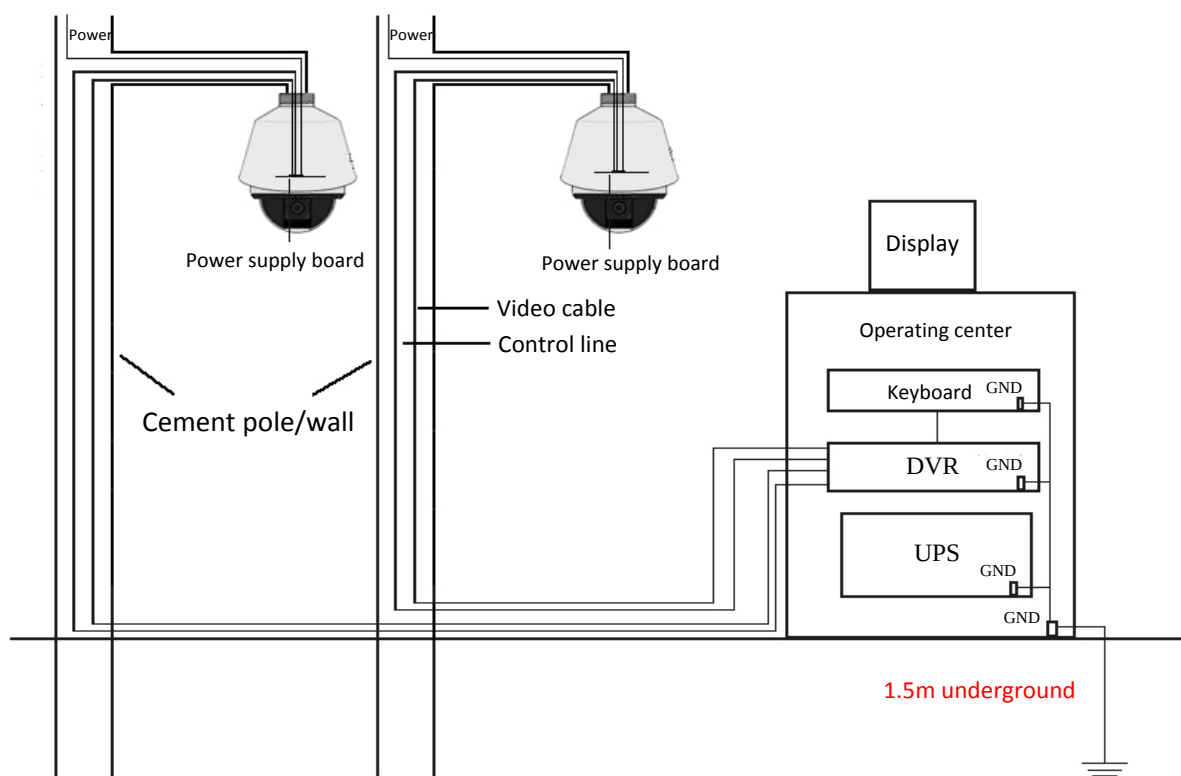


Figure A.3.2 Grounding in Cement Pole/Wall Installation

Notes:

- Because the signal transmission media of fiber optical camera and camera are isolated from the control center, they must be grounded locally to protect camera against damages.
- If the camera is installed in strong thunderstorm area, it must be grounded locally to release lightning or suchlike high energy to protect camera against damages. Refer to the following figure.

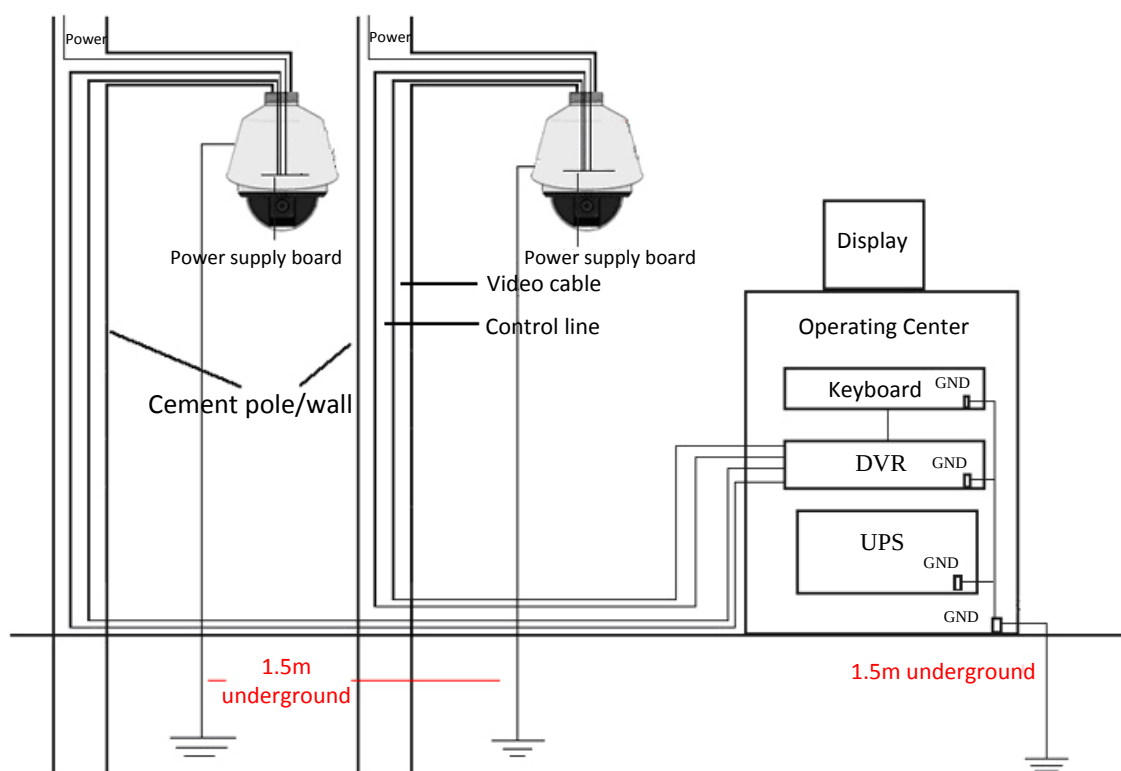


Figure A.3.3 Lightning-protection Grounding in Cement Pole/Wall Installation

Grounding for Metal Pole Installation:

When the camera is installed in environment where is conductive to the earth, e.g., metal pole, then the grounding of camera can be achieved by the properly grounded metal pole, meanwhile, the control center must be grounded locally as well. Refer to the following figure.

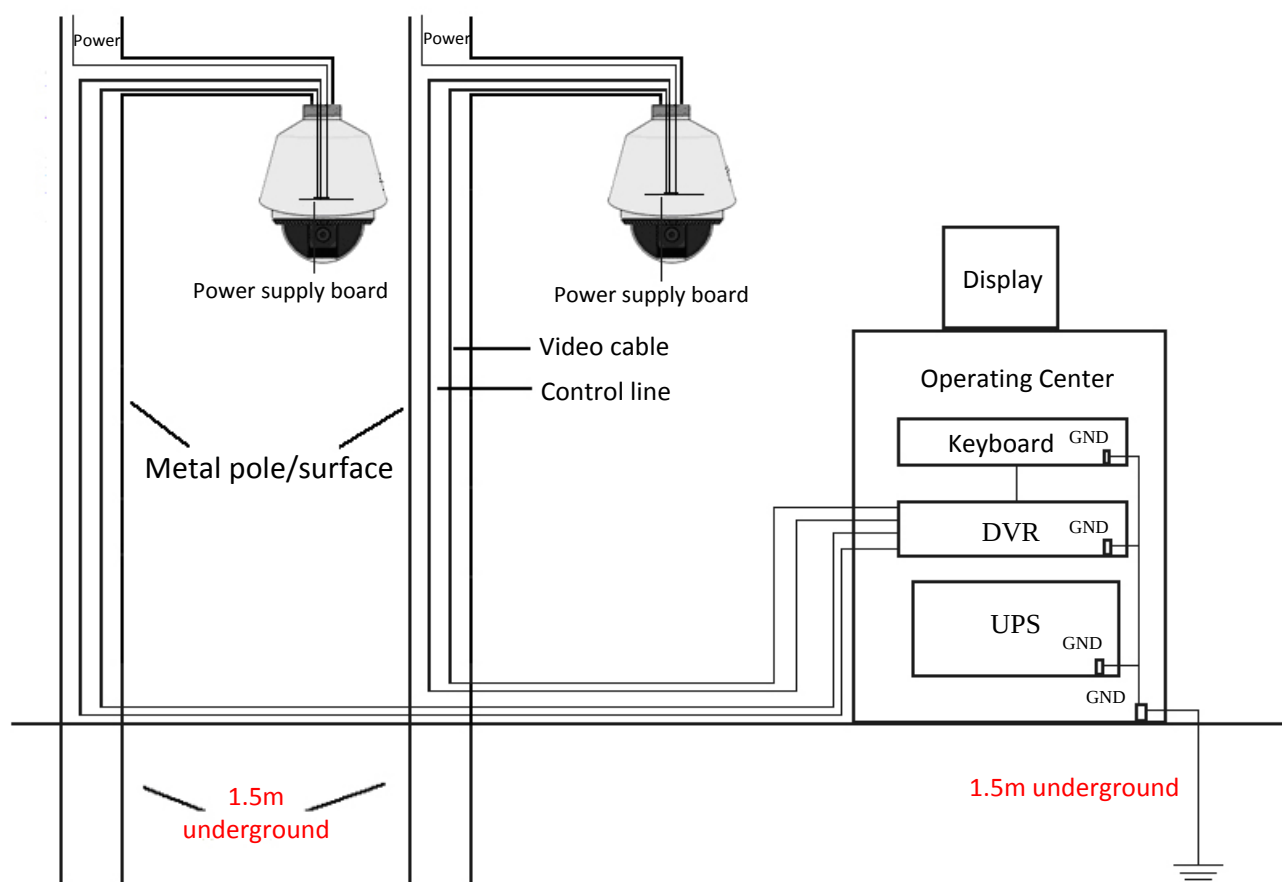


Figure A.3.4 Grounding in Metal Pole Installation

Note:

If the fiber optics, lightening protector or other device are applied during the transmission of camera, such devices as well as the video cables routing through must be proper grounded.

Appendix 3 Waterproof

Notes:

- The long-arm wall mount is recommended for the outdoor application of camera.
- You cannot use the short-arm wall mount or pendant mount for outdoor application, because it is not water-proof.
- It is recommended to use the mount with inner threaded interface and good waterproof performance.
- If you use a mount with outer threaded interface, adopt waterproof measures to the adapter applied between the mount and the camera.
- Do not install indoor camera to the outdoor environment.

L-shape Pole Mount

Make sure that the L-shape pole mount is designed with a certain inclination angle as shown in following figure. Water won't flow from the pole into the camera with the inclination angle.

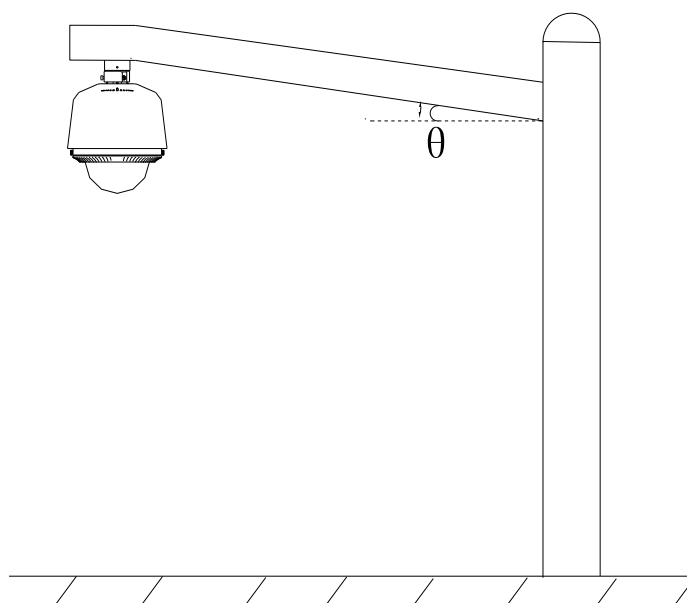


Figure A.4.1 Customized Mount

Appendix 4 Bubble Maintenance

The bubble is a transparent plastic. The dust, oil and finger print, etc. will cause scratch or image blur. Refer to the following method to clean the bubble.

- Handling dust

Use oil free soft brush or blowing dust ball to clean the dust.

- Handling oil

Steps:

1. Wipe off the water-drop or oil by soft cloth and dry the bubble.
2. Use oil free cotton cloth to wipe the bubble with alcohol or detergent.
3. Change the cloth to wipe the bubble until the bubble is clean.

Appendix 5 RS-485 Bus Connection

● General Property of RS-485 Bus

According to RS-485 industry bus standard, RS-485 is a half-duplex communication bus which has 120Ω characteristic impedance, the maximum load ability is 32 payloads (including controller device and controlled device).

● RS-485 Bus Transmission Distance

When using 0.56mm (24AWG) twisted-pair line, according to different baudrate, the maximum transmission distance theory table is shown as below:

Max. Distance of RS-485 Transmission	
Baudrate	Max Distance
2400BPS	1800m
4800BPS	1200m
9600BPS	800m

The transmission distance will be decreased if we use the thinner cable, or use this product under the strong electromagnetic interference situation, or there are lots of devices are added to the bus; on the contrary, the transmission distance will be increased.

● Connection Methods

RS-485 industry bus standard require daisy-chain connection method between any devices, both sides have to connect a 120Ω terminal resistance (show as Diagram 1), the simplified connection method is shown as diagram 2, but the distance of “D” should not be too long.

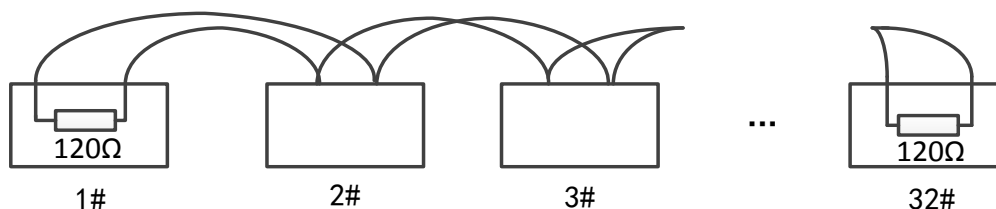


Figure A.6.1 RS-485 Connection 1

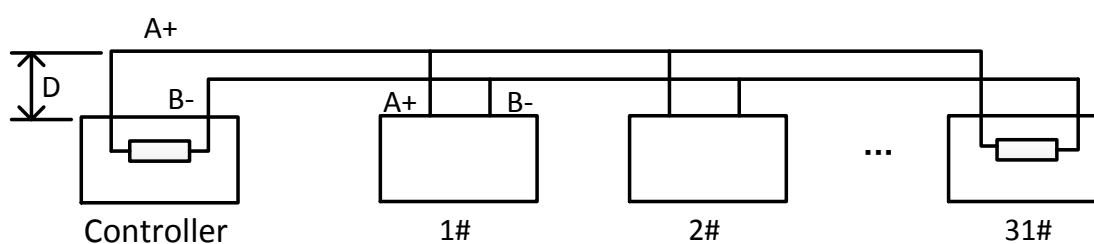


Figure A.6.2 RS-485 Connection 2

● Problems in the Practical Application

Normally, users adopt star-shape connection method in construction, under this situation, the terminal resistors must be connected between two farthest devices (as Figure A-9, 1# and 15#), but this connection method does not satisfy the requirement of the RS-485 industry standard so that it will lead to some problems such as signal reflection, anti-jamming ability decline when the devices are faraway. At this time, the camera will be uncontrollable, or self-running, etc.

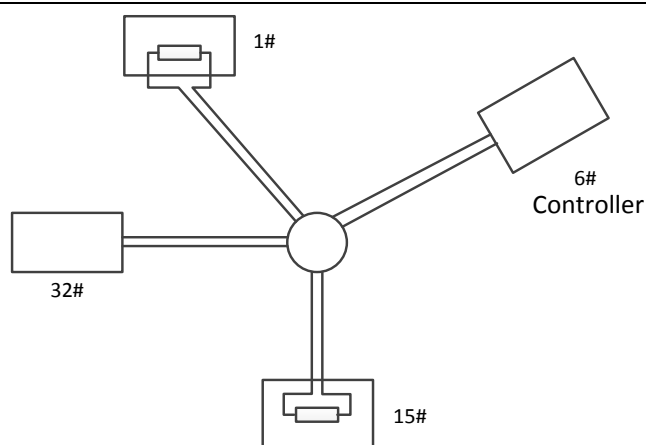


Figure A.6.3 Star Shape Connection

For such case, the best way is adding a RS-485 distributor. This product can effectively change the star-shape connection to which satisfies the requirement of RS-485 industry standard, in order to avoid those problems and improve the communication reliability. Refer to the following figure.

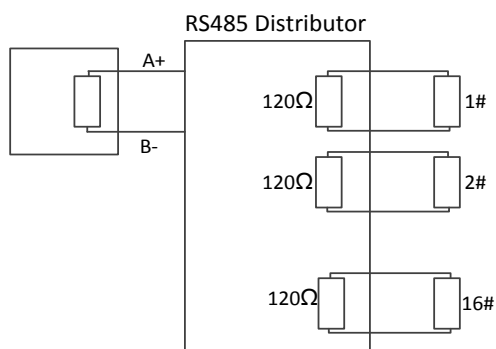


Figure A.6.4 RS-485 Distributor

● Troubleshooting of RS-485 communication

Problem	Possible Reasons	To Solve the Problem
The camera does the self-test action but cannot be controlled remotely.	1. The address or baudrate of the camera does not match with those of remote control device.	1. Adjust the address and baudrate of the remote control device to match with those of the camera.
	2. The wire RS-485+ connects to the interface RS-485- and wire RS-485- connects to the interface RS-485+.	2. Connect the wire RS-485+ to the interface RS-485+ and wire RS-485- to the interface RS-485-.
	3. The RS-485 wire is disconnected.	3. Reconnect the RS-485 wire tightly.
	4. RS-485 wire is broken.	4. Change a RS-485 wire.
The camera can be controlled but not smoothly.	1. The connection is loose.	1. Reconnect the RS-485 wire tightly.
	2. RS-485+ or RS-485-wire is broken.	2. Change a RS-485 wire.
	3. The camera is too far away from the remote control device.	3. Add a terminal resistor.
	4. Too many cameras are connected.	4. Add a RS-485 distributor.

Appendix 6 24VAC Wire Gauge & Transmission Distance

The following table describes the recommended max. distance adopted for the certain wire gauge when the loss rate of 24VAC voltage is less than 10%. For the AC driven device, the maximum voltage loss rate is 10% allowable. For example, for a device with the rating power of 80VA which is installed at a distance of 35 feet (10m) away from the transformer, then 0.8000mm is required as the minimum wire gauge.

Distance (feet) Wire Gauge (mm) Power (va)	0.8000	1.000	1.250	2.000
10	283(86)	451(137)	716(218)	1811(551)
20	141(42)	225(68)	358(109)	905(275)
30	94(28)	150(45)	238(72)	603(183)
40	70(21)	112(34)	179(54)	452(137)
50	56(17)	90(27)	143(43)	362(110)
60	47(14)	75(22)	119(36)	301(91)
70	40(12)	64(19)	102(31)	258(78)
80	35(10)	56(17)	89(27)	226(68)
90	31(9)	50(15)	79(24)	201(61)
100	28(8)	45(13)	71(21)	181(55)
110	25(7)	41(12)	65(19)	164(49)
120	23(7)	37(11)	59(17)	150(45)
130	21(6)	34(10)	55(16)	139(42)
140	20(6)	32(9)	51(15)	129(39)
150	18(5)	30(9)	47(14)	120(36)
160	17(5)	28(8)	44(13)	113(34)
170	16(4)	26(7)	42(12)	106(32)
180	15(4)	25(7)	39(11)	100(30)
190	14(4)	23(7)	37(11)	95(28)
200	14(4)	22(6)	35(10)	90(27)

Appendix 7 12VDC Wire Gauge & Transmission Distance

The following table describes the recommended max. distance adopted for the certain wire gauge when the loss rate of 12VDC voltage is less than 15%. For the DC driven device, the maximum voltage loss rate is 15% allowable.

Distance (feet) Wire Gauge (mm) Power (va)	0.800(20)	1.000(18)	1.250 (16)	2.000(12)
10	97(28)	153(44)	234(67)	617(176)
20	49(14)	77(22)	117(33)	308(88)
24	41(12)	64(18)	98(28)	257(73)
30	32(9)	51(15)	78(22)	206(59)
40	24(7)	38(11)	59(17)	154(44)
48	20(6)	32(9)	49(14)	128(37)
50	19(6)	31(9)	47(13)	123(35)
60	16(5)	26(7)	39(11)	103(29)
70	14(4)	22(6)	33(10)	88(25)
80	12(3)	19(5)	29(8)	77(22)
90	10.8(3.1)	17(5)	26(7)	69(20)
100	9.7(2.8)	15(4)	23(7)	62(18)
110	8.9(2.5)	14(4)	21(6)	56(16)
120	8.1(2.3)	13(4)	20(6)	51(15)
130	7.5(2.1)	11.8(3.4)	18(5)	47(14)
140	7(2)	11(3.1)	17(5)	44(13)
150	6.5(1.9)	10.2(2.9)	16(4)	41(12)
160	6.1(1.7)	9.6(2.7)	15(4)	39(11)
170	5.7(1.6)	9(2.6)	14(4)	36(10)
180	5.4(1.5)	8.5(2.4)	13(4)	34(10)

Appendix 8 Table of Wire Gauge Standards

Bare Wire Gauge(mm)	American Wire Gauge AWG	British Wire Gauge SWG	Cross-sectional Area of Bare Wire(mm ²)
0.750	21		0.4417
0.800	20	21	0.5027
0.900	19	20	0.6362
1.000	18	19	0.7854
1.250	16	18	1.2266
1.500	15	17	1.7663
2.000	12	14	3.1420
2.500			4.9080
3.000			7.0683

Appendix 9 Alarm In/Out Connections

Note:

This section is only for the cameras with alarm in/out functions.

The camera can be connected with alarm inputs (0~5VDC) and alarm outputs. Refer to the following diagrams for alarm output:

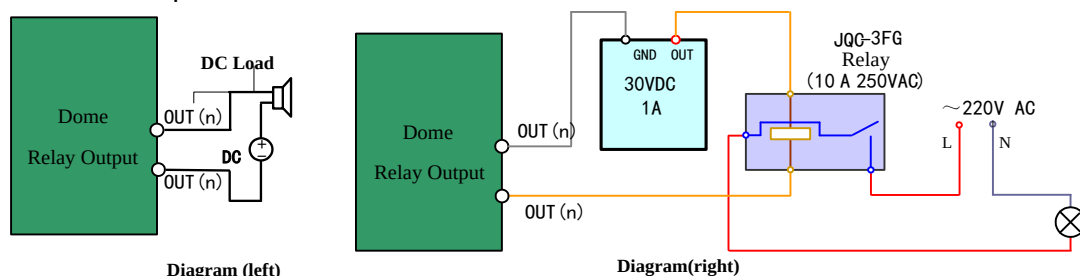


Figure A.9.1 Alarm Out Connections

The alarm provides the relay output (no voltage), and the external power supply is required when it connects to the alarm device.

- For DC power supply (left diagram), the input voltage must be no more than 30VDC, 1A.
- For AC power supply, the external relay must be used (right diagram) to prevent damages to the camera and avoid risk of electric shock.

Appendix 10 Camera Function Description

Note:

The functions vary depending on different camera models.

Limit Stops

The camera can be programmed to move within the limit stops (left/right, up/down).

Scan Modes

The camera provides 5 scan modes: auto scan, tilt scan, frame scan, random scan and panorama scan.

Preset Freezing

This feature freezes the scene on the monitor when the camera is moving to a preset. This allows for smooth transition from one preset scene to another. It also guarantees that masked area will not be revealed when the camera is moving to a preset.

Presets

A preset is a predefined image position. When the preset is called, the camera will automatically move to the defined position. The presets can be added, modified, deleted and called.

Label Display

The on-screen label of the preset title, azimuth/elevation, zoom, time and camera name can be displayed on the monitor. The displays of time and camera name can be programmed.

Auto Flips

In manual tracking mode, when a target object goes directly beneath the camera, the video will automatically flips 180 degrees in horizontal direction to maintain continuity of tracking. This function can also be realized by auto mirror image depending on the models of camera.

Privacy Mask

This function allows you to block or mask certain area of a scene, for preventing the personal privacy from recording or live viewing. A masked area will move with pan and tilt functions and automatically adjust in size as the lens zooms telephoto and wide.

3D Positioning

In the client software, use the left key of mouse to click on the desired position in the video image and drag a rectangle area in the lower right direction, then the camera system will move the position to the center and allow the rectangle area to zoom in. Use the left key of mouse to drag a rectangle area in the upper left direction to move the position to the center and allow the rectangle area to zoom out.

Proportional Pan/Tilt

Proportional pan/tilt automatically reduces or increases the pan and tilt speeds according to the amount of zoom. At telephoto zoom settings, the pan and tilt speeds will be slower than at wide zoom settings. This keeps the image from moving too fast on the live view image when there is a large amount of zoom.

Auto Focus

The auto focus enables the camera to focus automatically to maintain clear video images.

Day/Night Auto Switch

The cameras deliver color images during the day. And as light diminishes at night, the cameras switch to night mode and deliver black and white images with high quality.

Slow Shutter

In slow shutter mode, the shutter speed will automatically slow down in low illumination conditions to maintain clear video images by extending the exposure time. The feature can be enabled or disabled.

Backlight Compensation (BLC)

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. The BLC

(Backlight Compensation) function can compensate light to the object in the front to make it clear, but this causes the over-exposure of the background where the light is strong.

Wide Dynamic Range (WDR)

The wide dynamic range (WDR) function helps the camera provide clear images even under back light circumstances. When there are both very bright and very dark areas simultaneously in the field of view, WDR balances the brightness level of the whole image and provide clear images with details.

White Balance (WB)

White balance can remove the unrealistic color casts. White balance is the white rendition function of the camera to adjust the color temperature according to the environment automatically.

Patrol

A patrol is a memorized series of pre-defined preset function. The scanning speed between two presets and the dwell time at the preset are programmable.

Pattern

A pattern is a memorized series of pan, tilt, zoom, and preset functions. By default the focus and iris are in auto status during the pattern is being memorized.

Power Off Memory

The camera supports the power off memory capability with the predefined resume time. It allows the camera to resume its previous position after power is restored.

Time Task

A time task is a preconfigured action that can be performed automatically at a specific date and time. The programmable actions include: auto scan, random scan, patrol 1-8 ,pattern 1-4, preset 1-8,frame scan, panorama scan, tilt scan, day, night, reboot, PT adjust, Aux Output, etc.

Park Action

This feature allows the camera to start a predefined action automatically after a period of inactivity.

User Management

The camera allows you to edit users with different levels of permission, in the admin login status. Multiple users are allowed to access and control the same camera via network simultaneously.

3D Digital Noise Reduction

Comparing with the general 2D digital noise reduction, the 3D digital noise reduction function processes the noise between two frames besides processing the noise in one frame. The noise will be much less and the video will be clearer.

Dual-VCA

Combine the detected VCA information into the video stream, which can be used for the second-time analysis on the back-end device.



See Far, Go Further